Unit IX

COURSE TITLE Building Design for Homeland Security

TIME 150 minutes

UNIT TITLE Building Design Guidance

OBJECTIVES

1. Explain architectural considerations to mitigate impacts from blast effects and transmission of chemical, biological, and radiological agents from exterior and interior incidents
2. Identify key elements of building structural and nonstructural systems for mitigation of blast effects
3. Compare and contrast the benefit of building envelope, mechanical system, electrical system, fire protection system, and communications system mitigation measures, including synergies and conflicts
4. Apply these concepts to an existing building or building conceptual design and identify mitigation measures needed to reduce vulnerabilities

SCOPE

The following topics will be covered in this unit:

1. Architectural considerations, including building configuration, space design, and special situations
2. Building structural and nonstructural considerations with emphasis on progressive collapse, loads and stresses, and good engineering practices
3. Design issues for the building envelope, including wall design, window design, door design, and roof system design with approaches to define levels of protection
4. Mechanical system design issues, including interfacing with operational procedures, emergency plans, and training
5. Other building systems design consideration for electrical, fire protection, communications, electronic security, entry control, and physical security that mitigate the effects of a threat or hazard
6. Do an Activity that encompasses identified high risk pairs (asset – threat/hazard) in the threat-vulnerability matrix developed for the Case Study and select mitigation measures that reduce vulnerability and associated risk from the building perspective

REFERENCES

1. FEMA 426, Instructor Guide, and Student Manual.
2. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-1 to 3-46 and 3-48 to 3-52; Checklist at end of Chapter 1.
3. FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*
4. FEMA 430, *Primer for Incorporating Building Security Components in Architectural Design*
5. Case Study – Hazardville Information Company
6. Unit IX visuals

REQUIREMENTS

1. FEMA 426, pages 3-1 to 3-52
2. Unit IX visuals
3. Instructor Guide
4. Student Manual (one per student)
5. Overhead projector or computer display unit
6. Chart paper, easel, and markers

UNIT IX OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

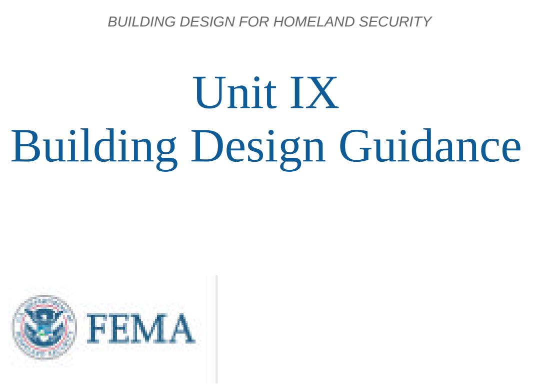
- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will continue the familiarization with the Case Study materials. The Case Study is a complete risk assessment and analysis of mitigation options and strategies for a typical commercial office building located in a mixed urban-suburban environment business park. The assessment will use the DoD Antiterrorism standards and the GSA Interagency Security Criteria to determine Levels of Protection and identify specific vulnerabilities. Mitigation options and strategies will use the concepts provided in FEMA 426 and other standard reference materials such as the RS Means Building Security: Strategy and Costs, NFPA 5000, and other FEMA publications related to emergency planning and disaster recovery.

- Refer students to their Student Manuals for worksheets and activities.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-1



Introduction and Unit Overview

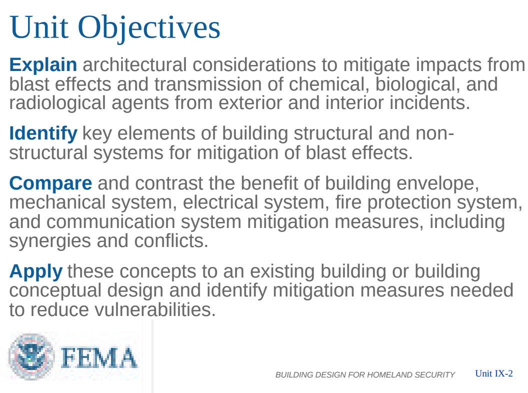
This is Unit IX Building Design Guidance. Continuing with our understanding of vulnerability and mitigation measures, we have looked at site and layout concerns and now turn our attention to what considerations are needed in building design to mitigate tactics involving explosive blast or CBR agents.

We will examine design considerations that achieve a balanced building envelope that provides a defensive layer against the given terrorist tactic and avoids creating ripple effects where one incident may affect more than one building system.

Catastrophic collapse of any building is a primary concern. Historically, the majority of fatalities that occur in terrorist attacks directed against buildings are due to building collapse. This was true for the Oklahoma City bombing in 1995 when 87 percent of the building occupants who were killed were in the collapsed portion of the Murrah Federal Building. But glass causes over 80 percent of injuries during bomb blast and there are some low cost techniques to keep CBR agents outside of buildings or to limit their spread inside.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-2



Unit Objectives

At the end of this unit, you should be able to:

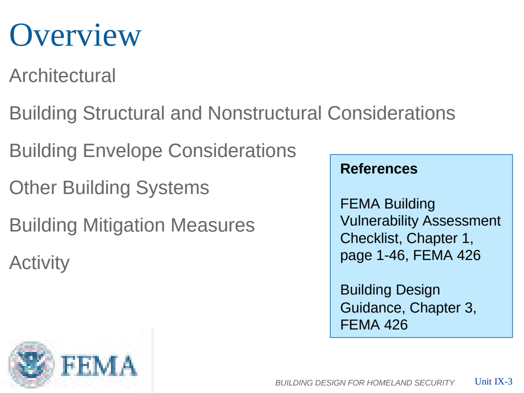
1. Explain architectural considerations due to impact from blast effects and transmission of chemical, biological, and radiological agents from exterior and interior incidents.

2. Identify key elements of building structural and nonstructural systems for mitigation of blast effects.

3. Compare and contrast the benefit of building envelope, mechanical system, electrical system, fire protection system, and communication system mitigation measures, including synergies and conflicts.

Apply these concepts to an existing building or building conceptual design and identify mitigation measures needed to reduce vulnerabilities.

VISUAL IX-3



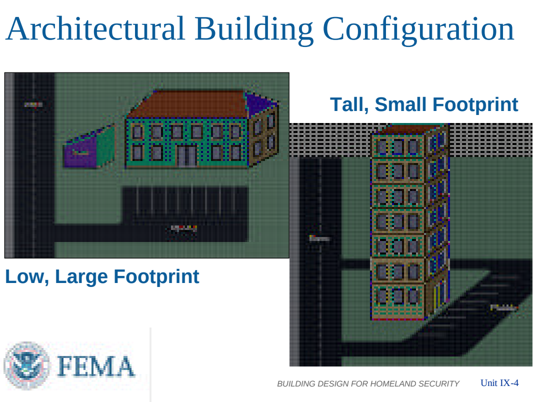
Overview

- Architectural
- Building Structural and Nonstructural Considerations
- Building Envelope Considerations
- Other Building Design Issues
- Building Mitigation Measures
- Activity

Note that one mitigation measure may reduce the risk of more than one asset – threat/hazard pair as illustrated by **Table 2-1 of FEMA 426**, where a mitigation measure may apply to multiple tactics.

INSTRUCTOR NOTES

VISUAL IX-4



CONTENT/ACTIVITY

Architectural Building Configuration (1)

Designers should balance a number of relevant considerations to the extent that site, economic, and other factors allow.

Some of the relevant considerations include the following:

- The shape of the building
- Low, large footprint buildings
- Tall, small footprint buildings

General benefits of the two basic approaches:

Low, Large Footprint:

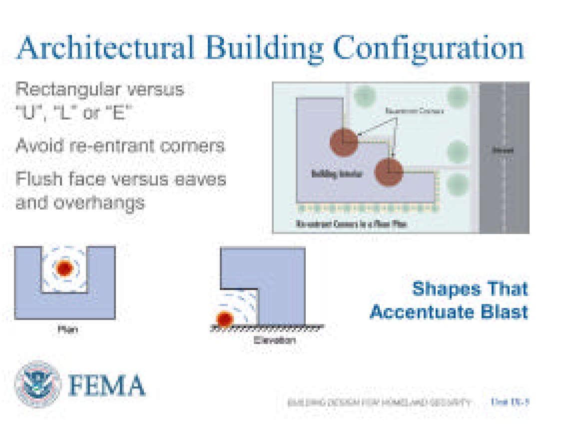
- Reduced effect of explosive blast (catches less of the blast wave)
- Reduced effect of progressive collapse (less of the building can fall)
- Reduced surveillance or easier mitigation (lower height allows terrain and landscaping options)
- Better energy conservation (green roof potential and earth-sheltered design)

Tall, Small Footprint:

- Reduced blast effects on upper floors
- Air intakes better protected against CBR events
- Site runoff reduced, reducing culvert size as a covert entry point

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL IX-5

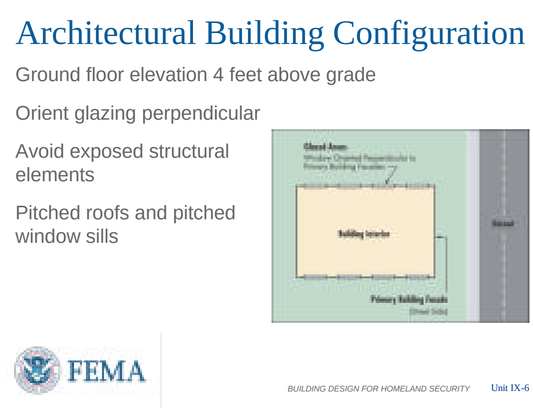


Architectural Building Configuration (2)

A lot can be done architecturally to mitigate the effects of a terrorist bombing on a facility. These measures often cost nothing or very little if implemented early in the design process. Future FEMA 430 will contain an expanded discussion of incorporating security components in architectural design.

- Further looking at building shapes, certain configurations trap the blast wave increasing overall damage to the structure. For example, "U" or "L" shaped buildings, overhangs, and re-entrant corners in general should be avoided.

VISUAL IX- 6

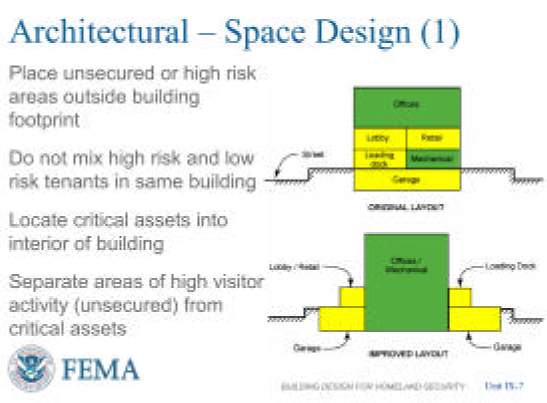


Architectural - Building Configuration (3):

- Elevating the ground floor makes moving vehicle attack more difficult
- If the glazing looks perpendicular to the direction of travel for the blast wave, the glass sees less reflected pressure.
- Do not have structural elements, like columns, easily exposed on the outside of the building. This goes for any architectural feature that can become damaged or disconnected by a blast wave.
- If armed attack includes Molotov cocktails or home-made grenades, pitched roofs and pitched window sills tend to cause the thrown item to roll off and away from the building. Air intakes have similar considerations.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL IX-7



Architectural - Space Design (1)

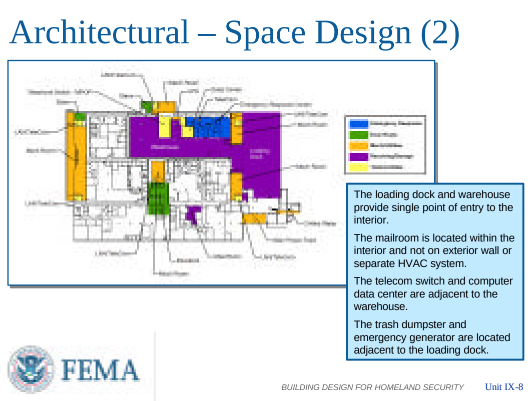
Unsecured areas should be physically separated from the main building to the extent possible.

For example, a separate lobby pavilion or loading dock outside the main footprint provides enhanced protection against damages and potential building collapse in the event of an explosion. Similarly, placing parking areas outside the main footprint of the building can be highly effective in reducing the vulnerability to catastrophic collapse.

The protection of the building interior can be divided into two categories:

- Functional layout
- Structural layout

VISUAL IX-8



Architectural - Space Design (2)

In terms of functional layout, public areas such as the lobby, loading dock, mail room, garage, and retail areas need to be separated from the more secured areas of the facility. This can be done by creating internal "hard lines" or buffer zones, using secondary stairwells, elevator shafts, corridors, and storage areas between public and secured areas.

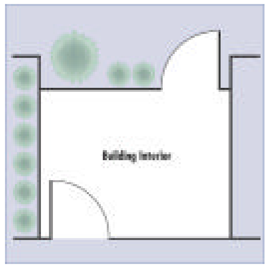
In lobby areas, the architect would be wise to consider the queuing requirements in front of the inspection stations so that visitors are not forced to stand outside during bad weather conditions or in a congested line inside a small lobby while waiting to enter the secured areas.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-9

Architectural – Space Design (3)

- Eliminate hiding places
- Interior barriers
- Offset doorways
- Minimize glazing, particularly interior glazing near high-risk areas



FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit IX-9

Architectural - Space Design (3)

In this slide, a range of design measures are presented that – when implemented – can increase the safety of the building's occupants from the effects of blast.

VISUAL IX-10

Architectural – Other Design Elements

- Safe havens
- Office locations
- Mixed occupancies
- Public toilets and service areas
- Retail uses in the lobby
- Stairwells
- Mailroom

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit IX-10

For additional information on safe havens, see FEMA 428.

Architectural - Other Design Elements

When designing high-risk buildings, engineers and architects should consider the following:

The innermost layer of protection within a physical security system is the **safe haven**. Safe havens are not intended to withstand a disciplined, paramilitary attack featuring explosives and heavy weapons.

Offices considered to be high risk (more likely to be targeted by terrorists) should be placed or glazed so that the occupants cannot be seen from an uncontrolled public area such as a street. Whenever possible, these spaces should face courtyards, internal sites, or controlled areas.

Mixed occupancies. High-risk tenants should not be housed with low-risk tenants. Terrorists may identify some targets based on their symbology, visibility, ideology, political views, potential for publicity, or simply the consequences of their loss.

Public toilets and service areas, or access to vertical circulation systems should not be

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

located in any non-secure areas, including the queuing area before visitor screening at the public entrance.

Retail and other mixed uses, which have been encouraged in public buildings by the Public Buildings Cooperative Use Act of 1976, create spaces that are open and inviting. Although important to the public nature of the buildings, the presence of retail and other mixed uses may present a risk to buildings and their occupants and should be carefully considered on a project-specific basis during project design.

Stairwells required for emergency egress should be located as remotely as possible from areas where blast events might occur and, wherever possible, should not discharge into lobbies, parking, or loading areas.

Mailroom should be located away from facility main entrances areas containing critical services, utilities, distribution systems, and important assets.

VISUAL IX-11

Progressive Collapse Design

Progressive collapse is a situation where local failure of a primary structural component leads to the collapse of adjoining members, which, in turn, leads to additional collapse. Hence, the total damage is disproportionate to the original cause. Progressive collapse is a chain reaction of structural failures that follows from damage to a relatively small portion of a structure. Information on progressive collapse can also be found in FEMA 427.

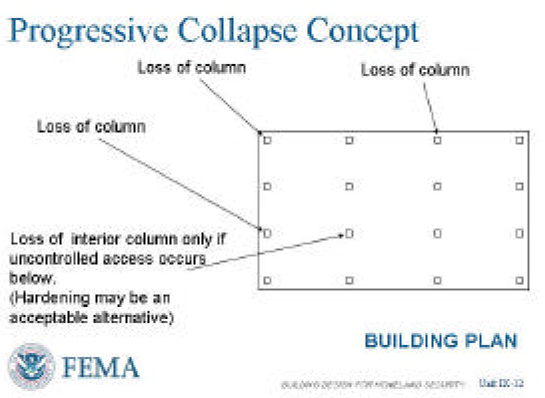
To minimize the potential for **progressive collapse**, designers should understand the following:

Buildings should be designed with the intent of reducing the potential for progressive collapse as a result of an abnormal loading event, regardless of the required level of

INSTRUCTOR NOTES

- The use of **redundant** lateral and vertical forces is highly encouraged.
- Ductile materials are needed for both primary and secondary structural elements to be capable of deforming well beyond the elastic limit.
- Both the primary and secondary structural elements should be designed to resist load reversals.
- Primary structural elements should be able to resist shear failures by having flexural capacity greater than shear capacity.

VISUAL IX-12



CONTENT/ACTIVITY

protection.

- Primary structural elements are columns girders and roof beams that are the first items for design to prevent progressive collapse.
- Secondary structural elements, such as floor beams and slabs, also may contribute to progressive collapse, such as by slenderizing a column due to loss of connections.
- Primary nonstructural elements, such as ceilings and heavy suspended mechanical equipment contribute to casualties but not progressive collapse.
- Secondary nonstructural elements, such as partitions, furniture, and light fixtures, like primary nonstructural elements also contribute to casualties, but not progressive collapse.

Progressive Collapse Concept

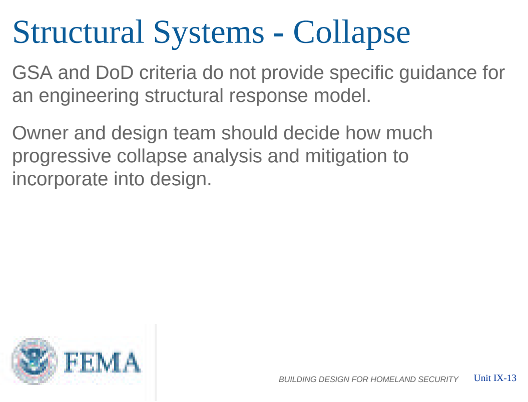
The GSA and DoD require that the structural response of a building be analyzed in a test that removes a key structural element (e.g., vertical load carrying column, section of bearing wall, beam, etc.) to simulate local damage from an explosion. If effective alternative load paths are available for redistributing the loads, originally supported by the removed structural element, the building has a low potential for progressive collapse.

- If a column is lost, will the rest of the building still stand?
- If an exterior beam is lost, will the rest of the building still stand?

If the threat can get to an interior column or beam, the same questions apply.

INSTRUCTOR NOTES

VISUAL IX-13



CONTENT/ACTIVITY

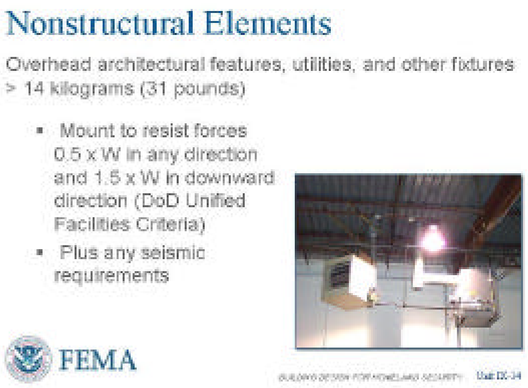
Structural System Collapse

- Although these criteria provide specific guidance on which structural elements must be analyzed for removal from the structural design configuration, they do not provide specific guidance for choosing an engineering structural response model for verifying the effectiveness of alternate load paths.
- Unless a building is being designed to meet the GSA or DOD criteria, it is up to the owner and the design team to decide how much progressive collapse analysis and mitigation to incorporate into their design.
- Priority should be given to the critical elements that are essential to mitigating the extent of collapse. Designs for secondary structural elements should minimize injury and damage.
- Consideration should be given to reducing damage and injury from primary as well as secondary nonstructural elements.

Both GSA and DoD take a threat-independent approach to progressive collapse – it does not matter how big the explosive weapon is, the building will remain standing if a column or beam is removed.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-14

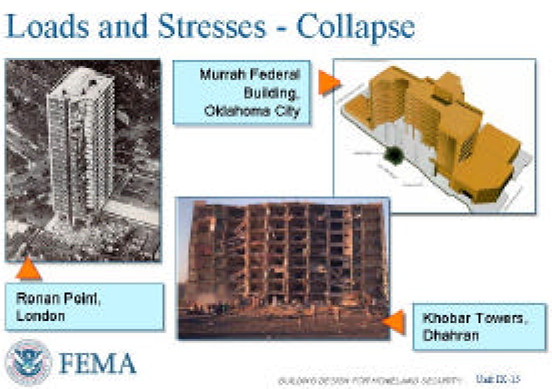


Nonstructural elements

False ceilings, light fixtures, venetian blinds, ductwork, air conditioners, and other equipment may become flying debris in the event of an explosion.

Wherever possible, it is recommended that the design be simplified to limit these hazards. Placing heavy equipment such as air conditioners near the floor rather than the ceiling is one idea; using curtains rather than Venetian blinds, and using exposed duct works as an architectural device are others.

VISUAL IX-15



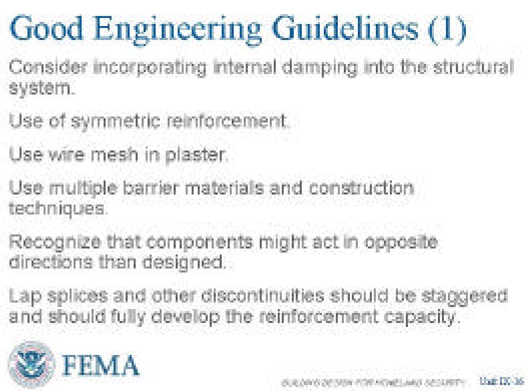
Loads and Stresses - Collapse

Structures should be designed to resist blast loads. The DoD designates the level of blast protection a building must meet based on how many occupants it contains and its function. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads.

Ronan Point had a whole section of the building collapse due to one wall in one apartment being lost. That changed the British Code to prevent that occurrence. Khobar Towers was designed to the British Code, and only the façade was lost. The Murrah Federal Building was not designed to the British Code and the loss of one column then affected a transfer girder due to discontinuities in columns across the lobby, resulting in load transfers that the building could not handle.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL IX-16

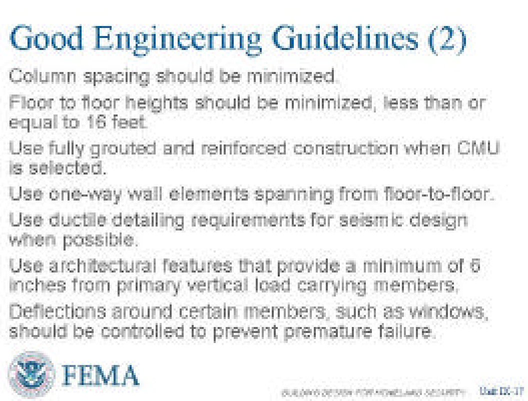


Good Engineering Guidelines (1)

The following guidelines are commonly used to mitigate the effects of blast on structures and to mitigate the potential for progressive collapse. These guidelines are not meant to be complete, but are provided to assist the designer in the initial evaluation and selection of design approaches. For example:

- Consider incorporating internal damping into the structural system to absorb the blast impact. While mass has been the blast design approach in the past, using more ductile materials with damping is being investigated.
- The use of symmetric reinforcement can increase the ultimate load capacity of the structure. This is especially true for load reversals on floor slabs.
- Consider wire mesh in plaster to reduce the incidence of flying fragments.
- Recognize that components might act in opposite directions than designed.
- Lap splices must be upgraded from those found in conventional construction to handle the forces during a blast event. Consider interlocking "J" splices.

VISUAL IX-17



Good Engineering Guidelines (2)

Additional good engineering practices include:

- A practical upper level for column spacing is 30 feet, 20 feet is better. If the column is lost, the remaining beam must span 40 to 60 feet. Above 60 feet, the beam becomes unreasonably large.
- In general, floor to floor heights should be minimized. Unless there is an overriding architectural requirement, a practical limit

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

is generally less than or equal to 16 feet. Consider bond beams, as used in seismic zones, to reduce the effective height of the wall.

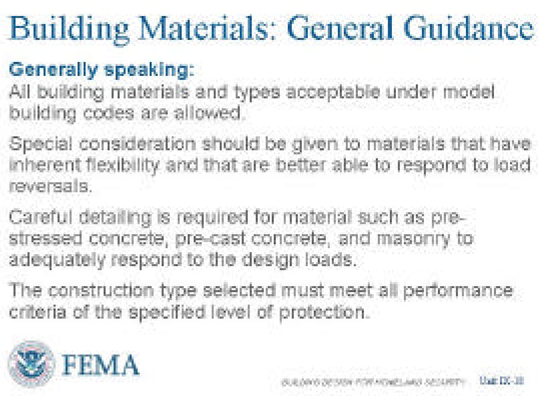
- Avoid the use of unreinforced masonry when blast is a threat. Masonry walls break up readily and become secondary fragments during blasts. Grout (mass) and reinforcement (ductility) are definitely required for blast resistance.
- Using one-way wall elements adds to prevention of progressive collapse. Although we are seeking a building envelope with balanced blast resistance, we would like the framing to be the last thing to fail.
- In many cases, the ductile detailing requirements for seismic design and the alternate load paths provided by progressive collapse design assist in the protection from blast.
- By keeping a 6-inch stand-off from vertical load carrying members, a small weapons charge is less likely to shear the member.
- The designer must bear in mind, however, that the design approaches are, at times, in conflict. These conflicts must be worked out on a case by case basis.

Finally, designers should note that:

- Deflections around certain members, such as windows, should be controlled to prevent premature failure. Additional reinforcement is generally required. Window frame deflection must not cause premature window glazing failure and window frame deflection must not differ greatly from the wall deflections. Seismic pinning of window frames may be required.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

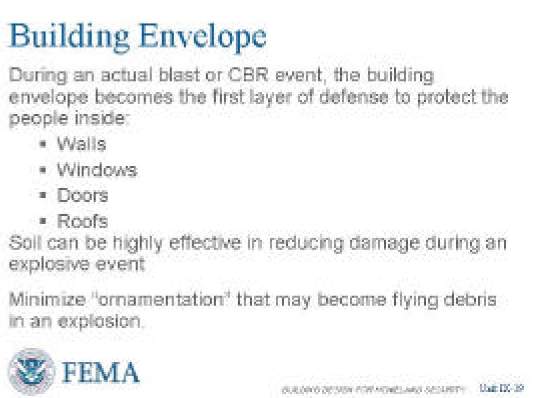
VISUAL IX-18



Building Materials: General Guidance

- All building materials and types acceptable under model building codes are allowed.
- Special consideration should be given to materials that have inherent flexibility and that are better able to respond to load reversals (i.e., cast in place reinforced concrete and steel construction).
- Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry (brick and concrete masonry unit) to adequately respond to the design loads. Even calling out seismic connections may not be adequate as the workforce may not be familiar with the changes from their norm – thus detailing is very important.
- The construction type selected must meet all performance criteria of the specified level of protection.

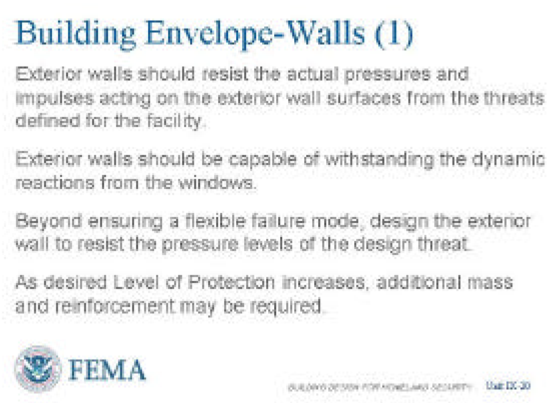
VISUAL IX-19



Building Envelope

INSTRUCTOR NOTES

VISUAL IX-20



Ideally, the exterior walls need to be able to resist the loads transmitted by the windows and doors. It is not uncommon for bullet-resistant windows to have a higher ultimate capacity than the walls to which they are attached.

Beyond ensuring a flexible failure mode, design the exterior wall to resist the pressure levels of the defined threat. Special reinforcing and anchors should be provided around blast-resistant window and door frames.

Poured-in-place reinforced concrete will provide the highest level of protection, but solutions like pre-cast concrete, reinforced CMU block, and metal studs may also be used to achieve lower levels of protection.

Thus, while the structural framing is the first consideration to prevent progressive collapse, the exterior walls are the second consideration to ensure blast pressure and fragmentation do not readily enter the building.

CONTENT/ACTIVITY

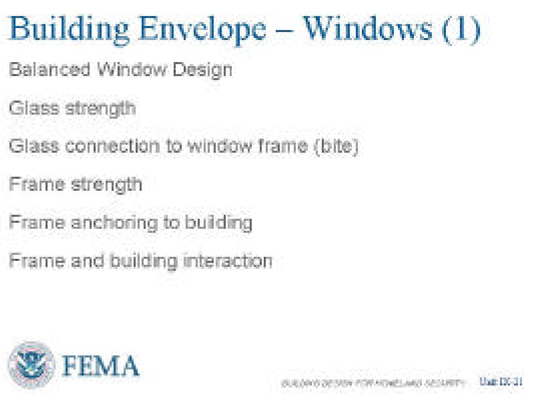
Building Envelope – Walls (1)

General principles:

- The exterior envelope of the building is the most vulnerable to an exterior explosive threat because it is closest to the blast.
- The exterior envelope also impacts the infiltration of CBR agents into the structure, but tight building construction must be done in conjunction with other actions to ensure some level of protection
- Soil can be highly effective in reducing the impact of a major explosion by reducing fragmentation off walls and street furniture or directing a blast wave over a building.
- Minimize "ornamentation" that may become flying debris in an explosion. This includes street furniture, overhangs, sculptures, etc.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL IX-21



Building Envelope – Windows (1)

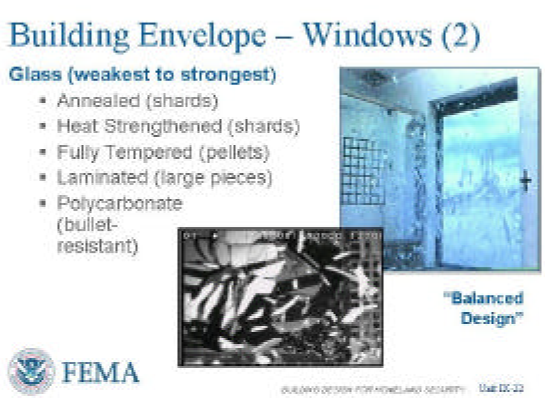
Window systems on the exterior façade of a building should be designed to mitigate the hazardous effects of flying glass during an explosion event. Designs should integrate the features of the glass, connection of the glass to the frame (bite), and anchoring of the frame to the building structure to achieve a "balanced design." This means all the components should have compatible capacities and theoretically would all fail at the same pressure-pulse levels. In this way, the damage sequence and extent of damage are controlled.

Ultimately, in a "balanced" design, the order of failure should be:

- Glass
- Window frame
- Frame anchoring
- Wall
- Building structural framing

The pressure differences should not be large and the Level of Protection for the Design Basis Threat should be met.

VISUAL IX-22



Building Envelope – Windows (2)

Five types of glass are commonly used in window glazing systems: annealed glass, heat strengthened glass, fully thermally tempered, laminated glass, and polycarbonate. Other types of glass materials exist, but are not commonly used in typical commercial window systems. Of the five common types, **annealed glass** and **fully thermally tempered glass** are the type of windows for most office buildings.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Annealed glass, also known as float, plate, or sheet glass, is the most common glass type used in commercial construction. Annealed glass is of relatively low strength and, upon failure, fractures into razor sharp, dagger-shaped fragments (see slide -- the right photo is annealed glass failing during an actual explosive test and the left photo is a closeup of the shards).

Heat strengthened glass (HS), also known as double strength glass, is used where wind loading starts becoming a problem. It breaks like annealed glass.

Fully thermally tempered glass (TTG) is typically four to five times stronger than annealed glass. Instead of shards, TTG breaks into pellets that can be stopped by a regular suit coat.

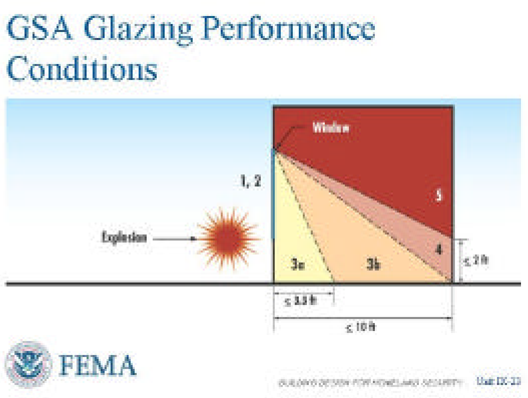
Laminated glass is a pane with multiple glass layers and a pliable interlayer material (usually made from polyvinyl butyral (PVB)) between the glass layers.

Thermoplastic polycarbonates are very strong and suitable for blast- and forced entry-resistant window design. They are usually laminated with glass on the outside to prevent environmental degradation of the plastic and aid in cleaning.

Wire-reinforced glass is a common glazing material. It consists of annealed glass with an embedded layer of wire mesh. It is usually used for fire resistance and as a forced entry barrier. It is not recommended for blast design.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-23

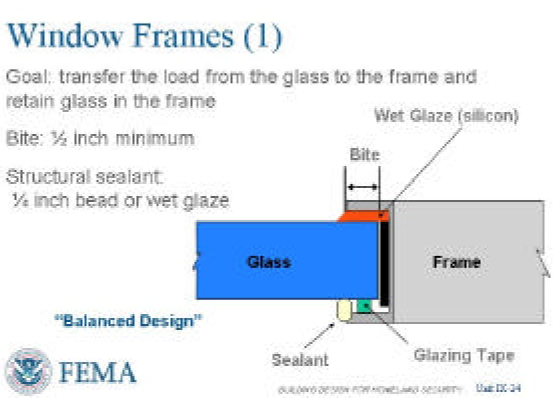


GSA Glazing Performance Conditions

Table 3-1 in FEMA 426 presents six GSA glazing protection levels based on how far glass fragments would enter a space and potentially injure its occupants (known as a flight model). This slide depicts how far glass fragments could enter a structure for each GSA performance condition. The divide between performance conditions 3a and 3b can be equated to the “threshold of injury.” The divide between performance conditions 4 and 5 can be equated to the “threshold of lethality.” A person standing in the room has a potential of being hit in the upper body/head area by glass fragments that are traveling fast enough to penetrate the body.

The GSA glazing performance conditions shown will correlate with the DoD levels of protection presented in **Table 3-2 in FEMA 426**.

VISUAL IX-24



Window Frames (1)

Window frames need to retain the glass so that the entire pane does not pull out (glass flexes and can pull out of frame during the blast) and also should be designed to resist the breaking stress of the window glass.

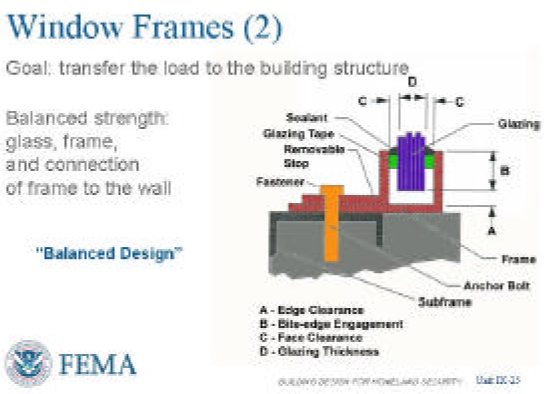
To retain the glass in the frame, a minimum of a 1/4-inch bead of structural sealant (i.e., silicone or polyvinyl butyral) should be used around the inner perimeter of the window. This should be done on all four sides of the window. Thus, strip windows with butt glazing are not good options as the bite must be large.

The window bite (i.e., the depth of window captured by the frame) needs to be at least 1/2 inch. DoD criteria calls for a minimum 3/8-

INSTRUCTOR NOTES	CONTENT/ACTIVITY

inch bite if silicon sealant is applied, but calls out a 1-inch bite if no silicone sealant is used. Butt glazed windows can require even more bite with or without sealant.

VISUAL IX-25



Window Frames (2)

The frame must not flex during the blast loading and cause the glass to pop out.

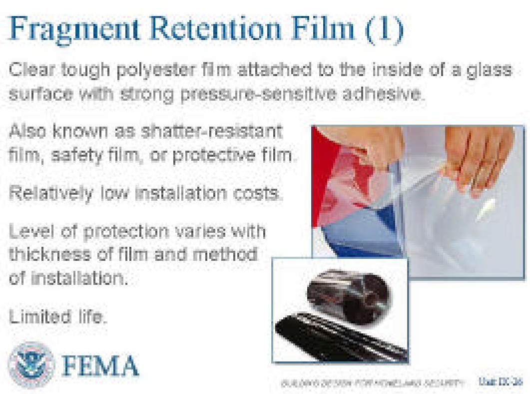
The blast loading across the glass and frame now transfers to the frame connections to the building. These connections must handle the shear and tensile stresses and the bending moments of the connection design.

The frame members connecting adjoining windows are referred to as mullions. These members may be designed using a static approach when the breaking strength of the window glass is applied to the mullion, or a dynamic load may be applied using the peak pressure and impulse values. Since mullions only connect at the ends to the building structure, the mullion must handle the transferred blast loading from both adjacent windows.

Other considerations for windows must balance the amount of light, energy conservation, noise transmission, venting of fumes, and emergency egress in addition to blast response and CBR protection.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL IX-26

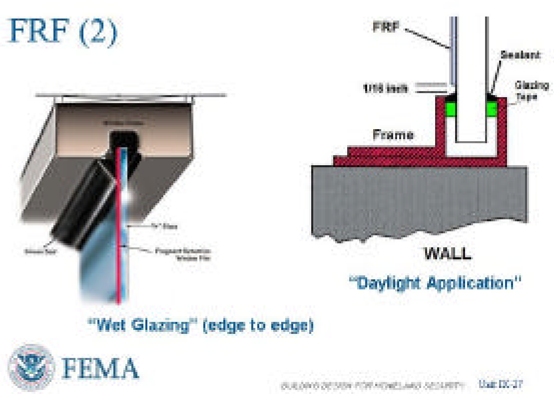


Fragment Retention Film (FRF) (1)

Another treatment used for mitigating the effects of an explosive attack is **security window film.** The polyester film used in commercial products is commonly referred to as fragment retention film (FRF), safety film, security film, protective film, or shatter-resistant film. These films are adhered to the interior surface of the window to provide fragment retention and reduce the overall velocity of the glass fragments at failure.

Fragment retention film combines a strong pressure sensitive adhesive with a tough polyester layer. It should be limited to use in retrofit applications due to degradation of the film and adhesive. Do not use for new construction.

VISUAL IX-27



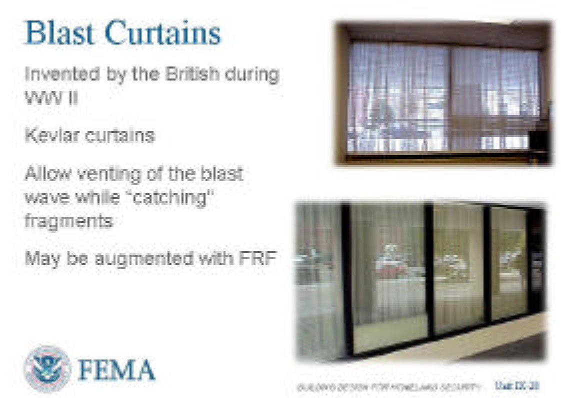
FRF (2)

Fragment retention film behaves similarly to relatively thin laminated and polycarbonate glazing in terms of fragmentation. It is available in common thicknesses of 2, 4, 7, and 10 mils. Also found up to 15 mils.

Fragment retention film improves the performance of the glass under blast loading to varying degrees, depending on the thickness, quality, and type of film installation. Note a daylight application will leave a 1/16 inch space around the edge of the FRF where water used to apply the FRF is squeegeed out. Daylight application of FRF to very thin glass can reduce the standoff distance in half for a given level of protection. The best performance is achieved when the film is installed into the bite of the glazing or is connected to the frame (mechanically or with chemical sealants).

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	Fragment retention film can also provide solar control benefits.

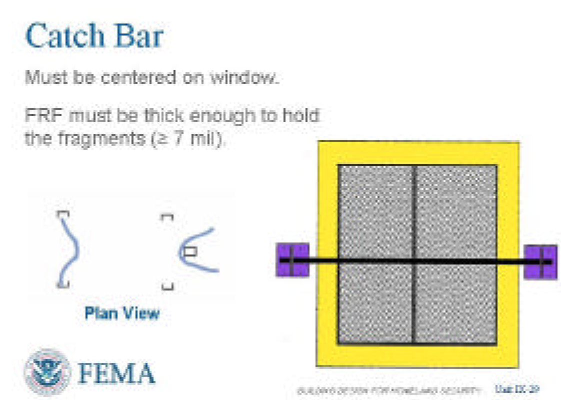
VISUAL IX-28



Blast Curtains

- Invented by the British during WWII
- Can now see out of these curtains as opposed to the "blackout" curtains from WWII by using Kevlar or other high strength fibers
- Allow venting of the blast wave while "catching" fragments
- May be augmented with FRF
- Connections of curtains or blast shields to building frame are critical

VISUAL IX- 29



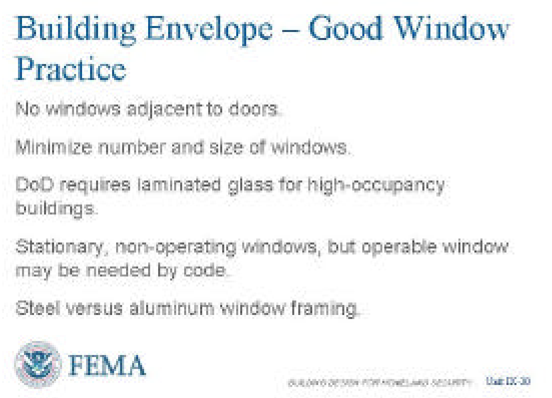
Catch Bar

Increased safety for fragment retention can be obtained in the event of catastrophic failure from an explosive blast by placing a decorative catchbar or grillwork on the interior of the glazing. Note, catchbars must be mounted across the center of mass of each window pane (vision area of glass) to be effective.

Catchbars are usually considered with a retrofit of fragment retention film to not only catch the glass, but also catch the existing window frame that may not be adequately connected to the wall. They can also be considered for laminated glass.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL IX-30



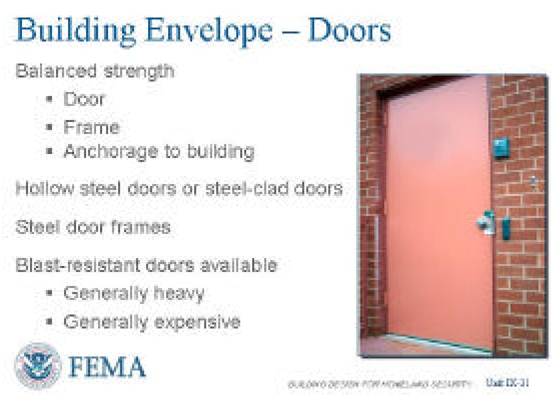
Building Envelope – Good Window Practice

The windows adjacent to doors allow easy access to the locking mechanism on the door.

Fewer and smaller windows limit cost and reduce damage if failure during bomb blast occurs.

Heavy duty aluminum frames have performed well.

VISUAL IX-31



Building Envelope - Doors

A door system includes the door, frame, and anchorage to the building. As part of a balanced design approach, exterior doors in high risk buildings should be designed to withstand the maximum dynamic pressure and duration of the load from the design threat explosive blast. Other general door considerations are as follows:

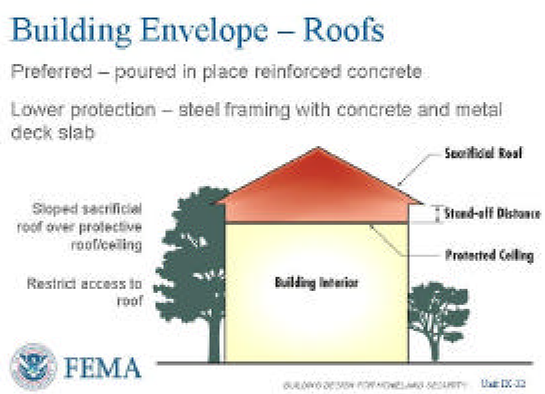
- Provide hollow steel doors or steel-clad doors with steel frames.
- Provide blast-resistant doors for high threats and high levels of protection.
- Limit normal entry/egress through one door, if possible.
- Keep exterior doors to a minimum while accommodating emergency egress.
- Ensure that exterior doors open outward from inhabited areas
- Replace externally mounted locks and hasps with internally locking devices because the weakest part of a door system is the latching component.
- Install doors, where practical, so that they present a blank, flush surface to the outside to reduce their vulnerability to

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

attack.

- Locate hinges on the interior or provide concealed hinges to reduce their vulnerability to tampering.
- Install emergency exit doors so that they facilitate only exiting movement.
- Equip any outward-opening double door with protective hinges and key-operated mortise-type locks.
- Provide solid doors or walls as a backup for glass doors in foyers.

VISUAL IX-32



Building Envelope – Roofs

For an explosive threat, especially for thrown explosives – satchels, hand grenades, and even mortars, the primary loading on the roof is downward over-pressure. The stand-off to the protected ceiling provides the protection. The sloped roof tends to cause the explosive to roll off and away from the building. For explosions at ground level, secondary loads include upward pressure due to the blast penetrating through openings and upward suction during the negative loading phase. The upward pressures may have an increased duration due to multiple reflections of the air blast internally. It is conservative to consider the downward and upward loads separately.

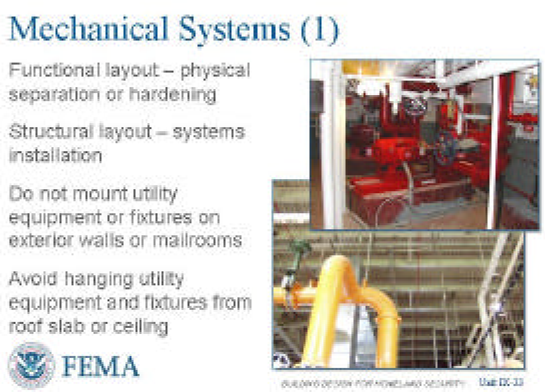
The preferred system is to use poured-in-place reinforced concrete with beams in two directions. If this system is used, beams should have stirrups along the entire span spaced not greater than one half the beam depths.

Less desirable systems include metal plate systems without concrete, and precast and pre/post tensioned systems.

Precast panels are problematic because of the tendency to fail at the connections.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-33



Mechanical system design standards address limiting damage to critical infrastructure and protecting building occupants against CBR threats.

- Controlling access to building information, including the operation of the mechanical systems, should be a security priority. This information could aid a terrorist attack.
- Finally, preventive maintenance that ensures the mechanical systems will work

Pre/post tensioned systems tend to fail in a brittle manner if stressed beyond their elastic limit and they also are not able to accept upward loads without additional reinforcement.

Many conventional roof designs will provide a suitable blast response for most buildings, considering minimum Design Basis Threats. The intent here is to point out what roofs may be a problem and why. For higher Design Basis Threats and tactics involving the roof, the protected ceiling and sacrificial roof concept applies.

Mechanical Systems (1)

The primary goal of a mechanical system after a terrorist attack should be to continue to operate key life safety systems. This can be accomplished by locating components in less vulnerable areas, limiting access to mechanical systems, and providing a reasonable amount of redundancy.

Designers should consider the following:

- During an interior bombing event, smoke removal and control are of paramount importance. The designer should consider the fact that, if window glazing is hardened, a blast may not blow out windows, and smoke may be trapped in the building.

The following suggestions attempt to protect the mechanical systems during an explosive blast event, have backup, or generally prevent access to utilities lines:

- Do not mount plumbing, electrical fixtures, or utility lines on the inside of

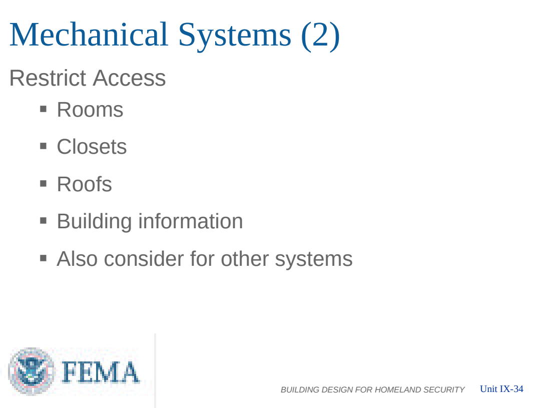
INSTRUCTOR NOTES	CONTENT/ACTIVITY

in all required modes must be done to ensure proper functioning after an event.

exterior walls, but, when this is unavoidable, mount fixtures on a separate wall at least 6 inches from the exterior wall face.

- Avoid plumbing on the roof slab.
- Avoid suspending plumbing fixtures and piping from the ceiling.
- Reduce the number of utility openings, manholes, tunnels, air conditioning ducts, filters, and access panels into the structure.
- Locate utility systems away from likely areas of potential attack, such as loading docks, lobbies, and parking areas.
- Protect building operational control areas and utility feeds to lessen the negative effects of a blast.
- Design operational redundancies to survive all kinds of attack.
- Use lockable systems for utility openings and manholes where appropriate. Infrequently used utility covers/manholes can be tack-welded as an inexpensive alternative to locking tamper-resistant covers.

VISUAL IX-34



Mechanical Systems (2)

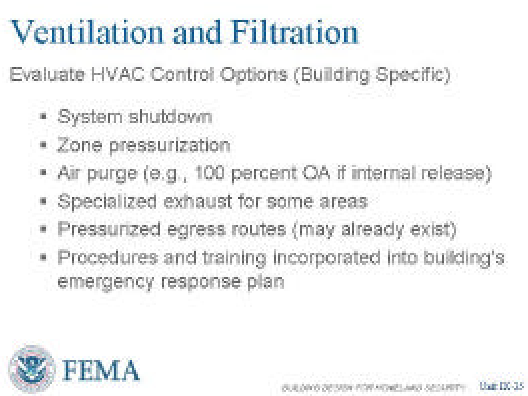
- Physical security for mechanical rooms to prevent the direct introduction of hazardous materials into the system of ducts that distributes air to the building should be maintained.
- Public access to building roofs should be prevented. Access to the roof may allow entry to the building and access to air intakes and HVAC equipment (e.g., self-contained HVAC units, laboratory or bathroom exhausts) located on the roof.
- Access to information on building operations (including mechanical, electrical, vertical transport, fire and life safety, security system plans and

INSTRUCTOR NOTES	CONTENT/ACTIVITY

schematics, and emergency operations procedures) should be strictly controlled.

- To prevent widespread dispersion of a contaminant released within lobbies, mailrooms, and loading docks, their HVAC systems should be isolated and the areas maintained at a negative pressure relative to the rest of the building, but at positive pressure relative to the outdoors.
- Large buildings usually have multiple HVAC zones, with each zone served by its own air handling unit and duct system.
- Consider “shelter-in-place” rooms or areas where people can congregate in the event of an outdoor release. The goal is to create areas where outdoor air infiltration is very low.

VISUAL IX-35



Ventilation and Filtration

Simplest to most complex in approaches to control the HVAC (heating, ventilating, and air conditioning) system during or after a terrorist attack.

- HVAC control may not be appropriate in all emergency situations. Protection from CBR attacks depends upon the design and operation of the HVAC system and the nature of the CBR agent release.
- Ducted returns offer limited access points to introduce a CBR agent. The return vents can be placed in conspicuous locations, reducing the risk of an agent being secretly introduced into the return system.
- A rapid response, such as shutting down an HVAC system, may involve closing various dampers, especially those controlling the flow of outdoor air (in the event of an exterior CBR release).
- Consideration should be given to installing low leakage dampers to

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

minimize this flow pathway.

VISUAL IX-36

Emergency Plans

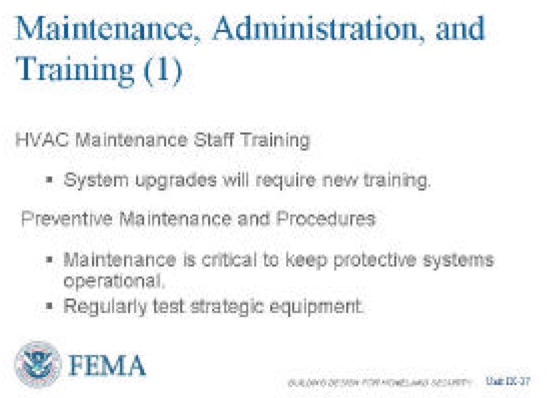
All buildings should have current **emergency plans** to address fire, weather, and other types of emergencies.

In light of past U.S. experiences with anthrax and similar threats, these plans should be updated to consider CBR attack scenarios and the associated procedures. Emergency plans should have procedures for communicating instructions to building occupants, identifying suitable shelter-in-place areas (if they exist), identifying appropriate use and selection of personal protective equipment (i.e., clothing, gloves, respirators), and directing emergency evacuations.

Building design should be able to ensure the optimal operation of the emergency plans. The emergency plans should not default to only what can be done after the building is constructed. In other words, like security and homeland defense, emergency planning should be an up-front design consideration that gets incorporated into the planning, budgeting, and design of the building.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

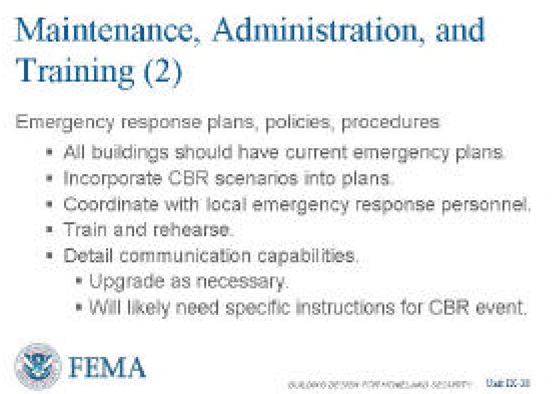
VISUAL IX-37



Maintenance, Administration, and Training (1)

In all cases, the HVAC Maintenance Staff must receive training in how the upgraded mechanical systems are designed to work, how they should be operated, and how they should be maintained and tested.

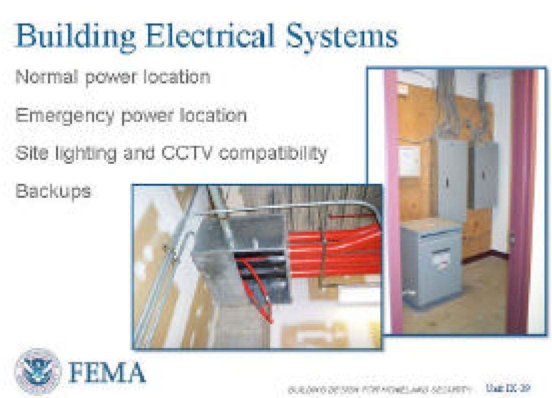
VISUAL IX-38



Maintenance, Administration, and Training (2)

- Training should be conducted
- Plans should be tested

VISUAL IX-39



Building Electrical Systems

The major security functions of the electrical system are to maintain power to essential building services, especially those required for life safety and evacuation; provide lighting and surveillance to deter criminal activities; and provide emergency communications. Designers should consider the following recommendations for buildings requiring high security:

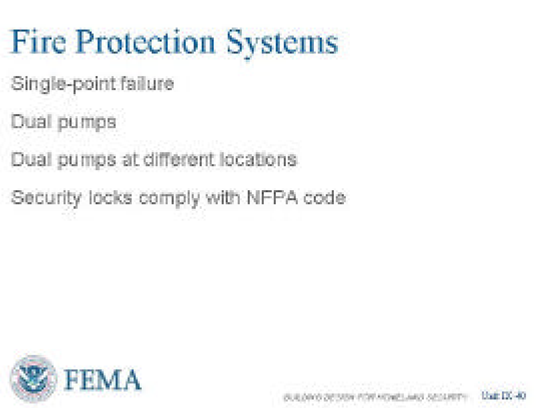
- Emergency and normal electric panels, conduits, and switchgear should be installed separately, at different locations,

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

and as far apart as possible.

- Emergency generators should be located away from loading docks, entrances, and parking.
- Fuel tanks should be mounted near the generator, given the same protection as the emergency generator, and sized to store an appropriate amount of fuel.
- Conduits and lines should be installed outside to allow a trailer-mounted generator to connect to the building's electrical system.
- Site lighting should be coordinated with the CCTV system.
- Emergency power should be provided for emergency lighting in restrooms.
- Building access points should be illuminated to aid in threat detection.
- Self-contained battery lighting will be in stairwells and for exit signs.
- Suspending electrical conduits from the ceiling should be avoided.
- Adequate lighting of perimeters and parking areas should be provided to aid in visual surveillance and to support the use of physical security systems.

VISUAL IX-40



Fire Protection Systems

The fire protection system inside the building should maintain life safety protection after an incident and allow for safe evacuation of the building when appropriate. To enhance the performance of fire protection systems, especially in the case of an explosive blast, the designer should consider the following:

- The fire protection water system should be protected from single-point failure in case of a blast event – maintain 50-foot separation from high risk areas (loading dock, lobby, etc.)
- To increase the reliability of the fire

INSTRUCTOR NOTES	CONTENT/ACTIVITY

protection system in strategic locations, a dual pump arrangement should be considered, with one electric pump and one diesel pump.

- The pumps should be located away from each other.
- All security locking arrangements on doors used for egress must comply with requirements of the National Fire Protection Association (NFPA) 101, Life Safety Code.

VISUAL IX-41

Communications Systems

For buildings requiring greater protection, the designer should consider the following:

Redundant communications. The facility could have a second telephone service to maintain communications in case of an incident. A base radio communication system with an antenna should be installed in the stairwell, and portable sets distributed on floors. This is the preferred alternative.

Radio telemetry. Distributed antennas could be located throughout the facility if required for emergency communications through wireless transmission of data.

Alarm and information systems. Alarm and information systems should not be collected and mounted in a single conduit, or even collocated. Circuits to various parts of the building should be installed in at least two directions and/or risers.

Empty conduits. Empty conduits and power outlets can be provided for future installation of security control equipment.

Mass notification. All inhabited buildings should have a timely means to notify occupants of threats and give instructions as to responses.

INSTRUCTOR NOTES

VISUAL IX-42

Chapter 3 of FEMA 426 is not a design guide for Electronic Security Systems (ESS). The following criteria are only intended to stress those concepts and practices that warrant special attention to enhance public safety. Consult design guides pertinent to the specific project for detailed information about electronic security. A description of Electronic Security Systems is provided in **Appendix D of FEMA 426.**

For control centers and building management systems, designers should consider the following:

- The Operational Control Center (OCC), Fire Command Center (FCC), and Security Control Center (SCC) may be collocated. If collocated, the chain of command should be carefully pre-planned to ensure the most qualified leadership is in control for specific types of events. Secure information links should be provided between the OCC, FCC, and SCC.
- A Backup Control Center (BCC) should be provided in a different location, such

CONTENT/ACTIVITY

Electronic Security Systems

The purpose of electronic security is to improve the reliability and effectiveness of life safety systems, security systems, and building functions. When possible, accommodations should be made for future developments in security systems.

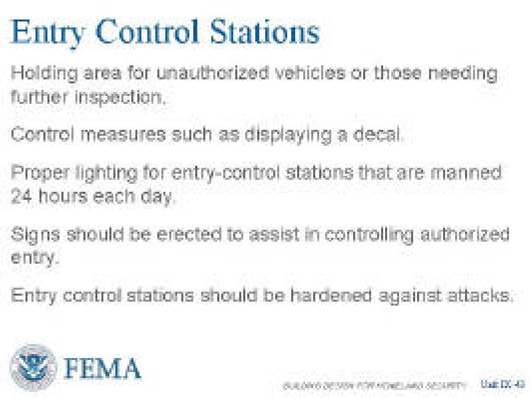
Electronic security, including surveillance, intrusion detection, and screening, is a key element of facility protection. Many aspects of electronic security and the posting of security personnel have been adequately dealt with in other criteria and guideline documents. These criteria primarily address access control design, including stair and lobby design, because access control must be considered when design concepts for a building are first conceived. Although fewer options are available for modernization projects, some designs can be altered to consider future access control objectives.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

as a manager's or engineer's office. If feasible, an off-site location should be considered.

- A fully redundant BCC should be installed (this is an alternative to the above).
- Basic intrusion detection devices should be provided: magnetic reed switches for interior doors and openings, glass break sensors for windows up to scalable heights, and balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors. Roof intrusion detection should be reviewed.
- Monitoring should be at an off-site facility.
- An on-site monitoring center should be used during normal business hours and be operational 24 hours.
- A Color CCTV surveillance system with recording capability should be provided to view and record activity at the perimeter of the building, particularly at primary entrances and exits.

VISUAL IX-43



Entry Control Stations

Entry control stations should be provided at main perimeter entrances of the building where security personnel are present (see **Figure 3-12 of FEMA 426**). In addition, entry control stations should be located close to the perimeter entrance to permit people inside the entry control station to maintain constant surveillance over the entrance and its approaches. Note that many of the considerations for entry control stations listed here are appropriate for Site and Layout Design as discussed in **Chapter 2 of FEMA 426**. Additional considerations at entry control stations include:

- A holding area for unauthorized vehicles

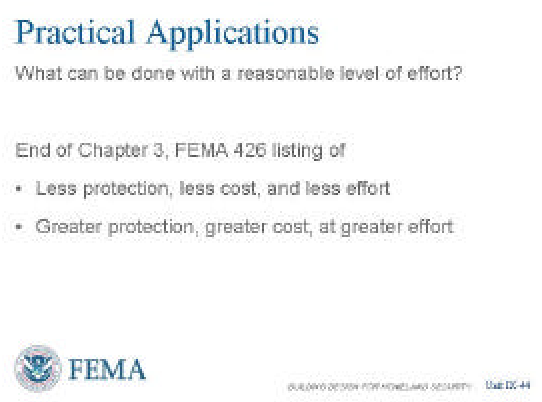
INSTRUCTOR NOTES	CONTENT/ACTIVITY

or those needing further inspection should be established. A turnaround area should be provided so that traffic is not impeded. This area should not be near the building (s) being protected.

- Control measures such as displaying a decal on the window or having a specially marked vehicle should be established.
- Entry control stations that are manned 24 hours each day should have interior and exterior lighting, interior heating (where appropriate), and a sufficient glassed area to afford adequate observation for people inside.
- Signs should be erected to assist in controlling authorized entry, to deter unauthorized entry, and to preclude accidental entry.
- The size and coloring of a sign, its letters, and the interval of posting must be appropriate to each situation.
- Entry control stations should be hardened against attacks according to the type of threat. The methods of hardening may include:
- Reinforced concrete or masonry
- Steel plating
- Bullet-resistant glass
- Commercially fabricated, bullet-resistant building components or assemblies

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-44



Direct students to **Table 2-1 in FEMA 426**.

Practical Applications

What can be done with a reasonable level of effort?

There is a range of FEMA 426 mitigation efforts at a range of cost. Consult **Table 2-1 of FEMA 426** to understand the benefit of various mitigation efforts against a range of terrorist tactics.

VISUAL IX-45

Desired Building Protection Level

The assessment process described to this point should determine the level of protection sought for the building structure for the threat/hazard specific to the facility. Explosive blast threats usually govern building structural design for high risk buildings.

Some design approaches are threat independent, such as progressive collapse as we will see in the next slides.
In every case, seek to include a balance between all the different requirements to include in design.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IX-46

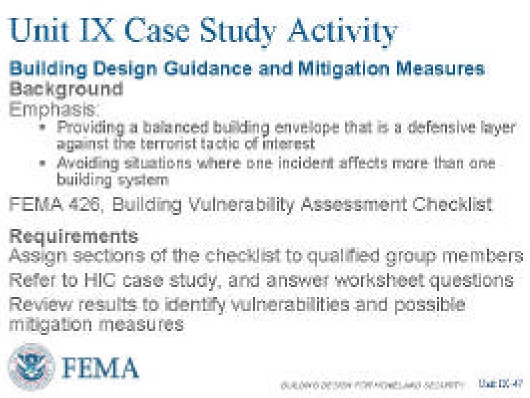
Summary

To summarize:

This course will provide a foundation for a systematic approach to assessing the vulnerabilities of your facilities to manmade hazards.

The **Building Vulnerability Assessment Checklist in FEMA 426** can provide an excellent framework for the identification of mitigation options that will – over time – significantly reduce the vulnerability of your facility to manmade hazards.

VISUAL IX-47



Refer participants to FEMA 426, the Unit IX Case Study activity in the Student Manual, and the vulnerability portfolio.

Members of the instructor staff should be available to answer questions and assist groups as needed.

At the end of 45 minutes, reconvene the class and facilitate group reporting.

Student Activity

The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary design vulnerability assessment.

The checklist includes questions that determine if critical systems will continue to function to enhance deterrence, detection, denial, and damage limitation, and emergency systems function during a threat or hazard situation.

Activity Requirements

- Continue working is small groups.
- Assign sections of the checklist to the group member who is most knowledgeable and qualified to perform an assessment of the assigned area.
- Refer to the HIC Case Study and to the GIS portfolio to determine answers to the worksheet questions.
- Then review results to identify

INSTRUCTOR NOTES

Many sections of the checklist are annotated "Unknown without a more detailed on-site assessment". As students review the Case Study materials and complete the checklist, in most cases, the "70 percent" solution is found without having to conduct the on-site assessment.

CONTENT/ACTIVITY

vulnerabilities and possible mitigation measures.

Take 45 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

Unit X will cover Electronic Security Systems.

UNIT IX CASE STUDY ACTIVITY:
BUILDING DESIGN GUIDANCE

In this Unit, the emphasis will be upon providing a balanced building envelope that is a defensive layer against the terrorist tactic of interest and avoiding situations where one incident affects more than one building system. The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment.

Requirement

Assign sections of the checklist to the group member who is most knowledgeable and qualified to perform an assessment of the assigned area. Refer to the HIC Case Study and to the vulnerability portfolio to determine answers to the questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the Building Vulnerability Assessment Checklist that address building design.

2. Upon completion of these portions of the checklist, refer back to the risk ratings determined in Unit V Case Study Activity and, based on this more detailed analysis, decide if the rating is accurate.

3. Select mitigation measures to reduce vulnerability and associated risk from building design.

4. Estimate the new risk ratings for high risk asset-threat pairs based on the recommended mitigation measures.

Section	Vulnerability Questions	Guidance	Observations
2.5	Do entrances avoid significant queuing?	If queuing will occur within the building footprint, the area should be enclosed in blast-resistant construction. If queuing is expected outside the building, a rain cover should be provided. For manpower and equipment requirements, collocate or combine staff and visitor entrances. Reference: *GSA PBS-P100*	
2.6	Does security screening cover all public and private areas? Are public and private activities separated?	Retail activities should be prohibited in non-secured areas. However, the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting buildings. Consider separating	Unknown without a more detailed on-site assessment.

	Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?	entryways, controlling access, hardening shared partitions, and special security operational countermeasures. References: *GSA PBS-P100 and FEMA 386-7*	
2.7	Is access control provided through main entrance points for employees and visitors? (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Within HIC, access control, lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, and electronic access control systems are all present. Access control at other companies within the complex is unknown.
2.8	Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?	Finishes and signage should be designed for visual simplicity. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	The building is monitored by door and window alarms, which connect to ADT, the nationwide alarm company. Unauthorized opening of any door or window will immediately notify ADT via telephone. ADT will normally call the HIC Security Office prior to contacting the police and DPS. HIC employees have proximity cards to allow them to enter the front and loading dock doors without activating the alarm. The innermost layer of physical security involves the Computer Data Center and the Communications Center. Equipped

			with locked doors, these two rooms meet the government's requirements for handling classified material. Only authorized employees possess the necessary proximity cards and PINs to gain access
2.9	Is access to elevators distinguished as to those that are designated only for employees and visitors?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	No elevators in HIC.
2.10	Do public and employee entrances include space for possible future installation of access control and screening equipment?	These include walk-through metal detectors and x-ray devices, identification check, electronic access card, search stations, and turnstiles. Reference: *GSA PBS-P100*	Yes, lobby area within HIC facility could accommodate space-saving screening equipment. Interior office space also has adequate room for such equipment.
2.11	Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?	Consider for exterior entrances to the building or to access critical areas within the building if explosive blast hazard must be mitigated. Reference: *U.S. Army TM 5-853*	The exterior walls are made of CMU with a brick veneer on the outside. Steel framework supports the structure, and exposed columns are enclosed in gypsum wallboard. Windows are double glazed, ¼ inch thick annealed glass. The construction of interior walls is unknown.
2.12	Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?	If the postulated threat in designing entrance access control includes rifles, pistols, or shotguns, then the screening area should have bullet-resistance to protect security personnel and uninvolved bystanders. Glass, if present, should also be bullet-resistant. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.

2.13	Do circulation routes have unobstructed views of people approaching controlled access points?	This applies to building entrances and to critical areas within the building. References: *USAF Installation Force Protection Guide and DoD UFC 4-010-01*	Yes.
2.14	Is roof access limited to authorized personnel by means of locking mechanisms?	References: *GSA PBS-P100 and CDC/NIOSH, Pub 2002-139*	Unknown without a more detailed on-site assessment.
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; Normal fuel storage; Main switchgear; Telephone distribution and main switchgear; Fire pumps; Building control centers; Uninterruptible Power Supply (UPS) systems controlling critical functions; Main refrigeration and ventilation systems if critical to building operation; Elevator machinery and controls; Shafts for stairs, elevators, and utilities; Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. Reference: *GSA PBS-P100*	Electrical service is provided through two buried transmission lines from two separate transformers outside the building. Emergency power is provided by a single diesel generator, located in a shed in the rear parking lot. The generator has a 50 gallon day tank, maintained at 80 percent capacity. The 2,000-gallon main tank is buried under the parking lot, near the generator. The diesel generator is configured to automatically start upon loss of commercial power to the Computer Center Bus. This happens about twice a year due to electrical storms or utility maintenance in the neighborhood. The backup diesel generator has never had to support HIC's power demands for longer than about 2 hours, and never with more than one chiller operating. It has never been tested for an extended period

			under heavy load. The batteries to support the UPS are in a small room next to the UPS room. Heating for the HIC building is provided by a combination of natural gas and electricity. This provides a regulated environment for the sensitive computer and communications equipment, and a comfortable environment for employees. Natural gas enters the building through two meters under the loading dock staircase and goes through the overhead to the mechanical and electrical (M&E) room at the building's southwest corner. Branches split off for two gas powered space heaters in the high-bay area by the loading dock. The main gas line goes to the main heater in the M&E room.
2.16	Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building. Reference: *GSA PBS-P100*	People are located along the exterior wall at the front of the building. The secure space has the best interior space location – not on an exterior wall, as does the conference room. The office space acts as the buffer between the critical functions in the back and the

			public area of the building at the main entrance.
2.17	Is high visitor activity away from critical assets?	High-risk activities should also be separated from low-risk activities. Also, visitor activities should be separated from daily activities. Reference: *USAF Installation Force Protection Guide*	All visitors enter through a common front entrance. Once admitted to the site, visitor activity is n/a.
2.18	Are critical assets located in spaces that are occupied 24 hours per day? Are assets located in areas where they are visible to more than one person?	Reference: *USAF Installation Force Protection Guide*	Unknown without a more detailed on-site assessment.
2.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?	Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against explosive blast. Consider a 50-foot separation distance in all directions. Reference: *GSA PBS-P100*	No, the loading dock connects directly into interior space, critical functions, and infrastructure.
2.20	Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets? Is the mailroom located near the loading dock?	The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief. By separating the mailroom and the loading dock, the collateral damage of an incident at one has less impact upon the other. However, this may be the preferred mailroom location. Off-site screening stations or a separate delivery processing building on site may be cost-effective, particularly if several buildings may share one mailroom. A separate delivery processing building reduces risk and simplifies protection	HIC has no mail room. Incoming mail is normally processed by the receptionist inside the front door. Large packages are delivered to the loading dock.

		measures. Reference: *GSA PBS-P100*	
2.21	Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?	Screening of all deliveries to the building, including U.S. mail, commercial package delivery services, delivery of office supplies, etc. Reference: *GSA PBS-P100*	HIC has no mail room.
2.22	Are areas of refuge identified, with special consideration given to egress?	Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards. Reference: *FEMA 386-7*	Yes, the Computer Data Center and the large conference room.
2.23	Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur? Are stairways maintained with positive pressure or are there other smoke control systems?	Consider designing stairs so that they discharge into other than lobbies, parking, or loading areas. Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc. out of the stairway. Pressurize exit stairways in accordance with the National Model Building Code. References: *GSA PBS-P100 and CDC/NIOSH, Pub 2002-139*	Emergency stairwells are located far from main stairwells. Unknown without a more detailed on-site assessment.
2.24	Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?	Egress pathways should be hardened and discharge into safe areas. Reference: *FEMA 386-7*	Unknown without a more detailed on-site assessment.
2.25	Do interior barriers differentiate level of security within a building?	Reference: *USAF Installation Force Protection Guide*	Electronic controls exist in the form of alarms, door locks, proximity cards, and use of PIN numbers for room/area access.
2.26	Are emergency systems located away from high-risk areas?	The intent is to keep the emergency systems out of harm's way, such that one incident takes out all capability – both the regular systems and their backups. Reference: *FEMA 386-7*	Emergency stairwells are located far from main stairwells. Emergency/backup generators are located away from main power supply lines; UPS is located inside the building's high bay area; exit

			doors are located throughout the site; natural gas enters the building under the loading dock stairwell.
2.27	Is interior glazing near high-threat areas minimized? Is interior glazing in other areas shatter-resistant?	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. Reference: *GSA PBS-P100*	Unknown without more detailed on-site assessment.
2.28	Are ceiling and lighting systems designed to remain in place during hazard events?	When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and nonstructural building components under loads not considered in standard building codes. It has been shown that connection criteria for these systems in high seismic activity areas resulted in much less falling debris that could injure building occupants. Mount all overhead utilities and other fixtures weighing 14 kilograms (31 pounds) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This standard does not preclude the need to design equipment mountings for forces required by other criteria, such as seismic standards. Reference: *DoD Minimum Antiterrorism Standards for Buildings*	Unknown without a more detailed on-site assessment.

3	**Structural Systems**		
3.1	What type of construction? What type of concrete and reinforcing steel?	The type of construction provides an indication of the robustness to abnormal loading and load reversals. A reinforced concrete moment-resisting frame provides	Located in a suburban office complex, the HIC office building comprises a 22,000

	What type of steel? What type of foundation?	greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or un-reinforced. A rapid screening process developed by FEMA for assessing structural hazards identifies the following types of construction with a structural score ranging from 1.0 to 8.5. A higher score indicates a greater capacity to sustain load reversals. Wood buildings of all types - 4.5 to 8.5 Steel moment-resisting frames - 3.5 to 4.5 Braced steel frames - 2.5 to 3.0 Light metal buildings - 5.5 to 6.5 Steel frames with cast-in-place concrete shear walls - 3.5 to 4.5 Steel frames with unreinforced masonry infill walls - 1.5 to 3.0 Concrete moment-resisting frames - 2.0 to 4.0 Concrete shear wall buildings - 3.0 to 4.0 Concrete frames with unreinforced masonry infill walls - 1.5 to 3.0 Tilt-up buildings - 2.0 to 3.5 Precast concrete frame buildings - 1.5 to 2.5 Reinforced masonry - 3.0 to 4.0 Unreinforced masonry - 1.0 to 2.5 References: *FEMA 154 and Physical Security Assessment for the Department of Veterans Affairs Facilities*	square foot main floor for offices and computers, and a 3,300 square foot executive mezzanine (a second floor over part of the office). The building that houses the Hazardville Information Company (HIC) is an office building of standard construction. The walls are made of CMU with a brick veneer on the outside. Steel framework supports the structure, and exposed columns are enclosed in gypsum wallboard. The roof is a metal deck with gravel on top and insulation underneath. It is slightly angled to allow water to drain. The roof overhangs the front entrance by 8 feet. This provides a covered area for employees to stay dry on rainy days. Cylindrical columns support the overhang. Windows are double glazed, ¼ inch thick annealed glass.
3.2	Do the reinforced concrete structures contain symmetric steel	Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.

	reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams and girders that may be subjected to rebound, uplift and suction pressures? Do the lap splices fully develop the capacity of the reinforcement? Are lap splices and other discontinuities staggered? Do the connections possess ductile details? Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?		
3.3	Are the steel frame connections moment connections? Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system? What are the floor-to-floor heights?	A practical upper level for column spacing is generally 30 feet. Unless there is an overriding architectural requirement, a practical limit for floor-to-floor heights is generally less than or equal to 16 feet. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.
3.4	Are critical elements vulnerable to failure?	The priority for upgrades should be based on the relative importance of structural or non-structural elements that are essential to mitigating the extent of collapse and minimizing injury and damage. Primary Structural Elements provide the essential parts of the building's resistance to catastrophic blast loads and	Unknown without a more detailed on-site assessment.

		progressive collapse. These include columns, girders, roof beams, and the main lateral resistance system. Secondary Structural Elements consist of all other load bearing members, such as floor beams, slabs, etc. Primary Nonstructural Elements consist of elements (including their attachments) which are essential for life safety systems or elements which can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units. Secondary Nonstructural Elements consist of all elements not covered in primary nonstructural elements, such as partitions, furniture, and light fixtures. Reference: *GSA PBS-P100*	
3.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?	The extent of damage to the structure and exterior wall systems from the bomb threat may be related to a protection level. The following is for new buildings: Level of Protection Below Antiterrorism Standards – Severe damage. Frame collapse/massive destruction. Little left standing. Doors and windows fail and result in lethal hazards. Majority of personnel suffer fatalities. Very Low Level Protection – Heavy damage. Onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into	The standard construction techniques used to build the site HIC occupies do not create buildings that withstand explosive blasts. Terrorist threat was not a part of design consideration.

		rooms, presenting serious hazards. Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities. Low Level of Protection – Moderate damage, unrepairable. Major deformation of non-structural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely. Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards. Majority of personnel suffer significant injuries. There may be a few (<10 percent) fatalities. Medium Level Protection – Minor damage, repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable. Some minor injuries, but fatalities are unlikely. High Level Protection – Minimal damage, repairable. No permanent deformation of primary and secondary structural members or non-structural elements. Glazing will not break. Doors will be reusable. Only superficial injuries are likely. Reference: *DoD UFC 4-010-01*	
3.6	Is the structure vulnerable to progressive collapse? Is the building capable of sustaining the removal of a column for one floor above	Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major	Unknown without a more detailed on-site assessment.

	grade at the building perimeter without progressive collapse? In the event of an internal explosion in an uncontrolled public ground floor area does the design prevent progressive collapse due to the loss of one primary column? Do architectural or structural features provide a minimum 6-inch standoff to the internal columns (primary vertical load carrying members)? Are the columns in the unscreened internal spaces designed for an unbraced length equal to two floors, or three floors where there are two levels of parking?	structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted. Reference: *GSA PBS-P100*	
3.7	Are there adequate redundant load paths in the structure?	Special consideration should be given to materials that have inherent ductility and that are better able to respond to load reversals, such as cast in place reinforced concrete, reinforced masonry, and steel construction. Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Primary vertical load carrying members should be protected where parking is inside a facility and the building superstructure is supported by the parking structure. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.
3.8	Are there transfer girders supported by columns within unscreened public spaces or at the exterior of	Transfer girders allow discontinuities in columns between the roof and foundation. This design has inherent difficulty in transferring load to redundant	Unknown without a more detailed on-site assessment.

	the building?	paths upon loss of a column or the girder. Transfer beams and girders that, if lost, may cause progressive collapse are highly discouraged. Reference: *GSA PBS-P100*	
3.9	What is the grouting and reinforcement of masonry (brick and/or concrete masonry unit (CMU)) exterior walls?	Avoid unreinforced masonry exterior walls. Reinforcement can run the range of light to heavy, depending upon the stand-off distance available and postulated design threat. Reference: *GSA PBS-P100* recommends fully grouted and reinforced CMU construction where CMU is selected. Reference: *DoD Minimum Antiterrorism Standards for Buildings* states "Unreinforced masonry walls are prohibited for the exterior walls of new buildings. A minimum of 0.05 percent vertical reinforcement with a maximum spacing of 1,200 mm (48 in) will be provided. For existing buildings, implement mitigating measures to provide an equivalent level of protection." [This is light reinforcement and based upon the recommended stand-off distance for the situation.]	Unknown without a more detailed on-site assessment.
3.10	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	Design the floor of the loading dock for blast resistance if the area below is occupied or contains critical utilities. Reference: *GSA PBS-P100*	No.
3.11	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment- resistant. Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside,	There is no mail room at this facility.

		but that readily fail and vent if exposed to blast pressure on the inside. Reference: *GSA PBS-P100*	

4	Building Envelope		
4.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	The performance of the façade varies to a great extent on the materials. Different construction includes brick or stone with block backup, steel stud walls, precast panels, or curtain wall with glass, stone, or metal panel elements. Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls should be considered primary structures and should resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration should be given to construction types that reduce the potential for injury. Reference: *GSA PBS-P100*	The exterior walls are made of CMU with a brick veneer on the outside. Steel framework supports the structure, and exposed columns are enclosed in gypsum wallboard. Windows are double glazed, ¼ inch thick annealed glass. The construction of interior walls is unknown. The level of protection provided by the buildings structure depends upon the blast exposure.
4.2	Is there less than 40 % fenestration openings per structural bay? Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.) Do the glazing systems with a ½-inch (3/4-inch better) bite contain an application of structural silicone? Is the glazing laminated or is it protected with an anti-shatter (fragment retention) film? If an anti-shatter film is used, is it a minimum of a	The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40 percent of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows; an architect may favor window curtain walls; building codes require so much fenestration per square footage of floor area; fire codes require a prescribed window opening area if the window is a designated escape route; and the building owner has cost concerns. Ideally, an owner would want 100 percent of the glazed area to provide the design protection level against the postulated	Windows are only used in the office space area of the building. While dimensions are not given, it looks like the glass is at least 40 percent of the wall area between building structural columns. The window system is a standard commercial installation and thus, the glass, framing, and anchorage is expected to be insufficient for the design basis threat at the available standoff. One benefit is that there are windows only on two sides of the building.

	7-mil thick film, or specially manufactured 4-mil thick film?	explosive threat (design basis threat– weapon size at the expected stand-off distance). However, economics and geometry may allow 80 percent to 90 percent due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher). Reference: GSA PBS-P100	
4.3	Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected? Are the walls capable of withstanding the dynamic reactions from the windows? Will the anchorage remain attached to the walls of the building during an explosive event without failure? Is the façade connected to back-up block or to the structural frame? Are non-bearing masonry walls reinforced?	Government produced and sponsored computer programs coupled with test data and recognized dynamic structural analysis techniques may be used to determine whether the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants. A breakage probability no higher than 750 breaks per 1,000 may be used when calculating loads to frames and anchorage. The intent is to ensure the building envelope provides relatively equal protection against the postulated explosive threat for the walls and window systems for the safety of the occupants, especially in rooms with exterior walls. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.
4.4	Does the building contain ballistic glazing? Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing? Does the building contain security-glazing? Does the security-glazing	Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material. If windows are upgraded to bullet-resistant, burglar-resistant, or forced entry-resistant, ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.

	meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material? Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?		
4.5	Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?	In-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures. These non-window openings should also be as secure as the rest of the building envelope against forced entry. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.

6	**Mechanical Systems (HVAC and CBR)**		
6.1	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?	Air intakes should be located on the roof or as high as possible. Otherwise secure within CPTED-compliant fencing or enclosure. The fencing or enclosure should have a sloped roof to prevent the throwing of anything into the enclosure near the intakes. Reference: *GSA PBS-P100* states that air intakes should be on the fourth floor or higher and, on buildings with three floors or less, they should be on the roof or as high as practical. Locating intakes high on a wall is preferred over a roof location. Reference: *DoD UFC 4-010-0*1 states that, for all new inhabited buildings covered by this document, all air intakes should be located at least 3 meters (10 feet) above the ground. Reference: *CDC/NIOSH*, *Pub 2002-139* states: "An extension height of 12 feet (3.7 m) will	The air used to heat or cool the HIC Headquarters building is filtered in the HVAC room using standard industrial grade filters. Outside air is brought in through a vent in the wall. The vent is alarmed to prevent intruder access. A screened exhaust duct is on the roof. Airflow throughout the building is through a series of ducts hidden in the ceiling of each area. The ducts are divided in half to allow them

		place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes". Reference: *LBNL PUB-51959:* Exhausts are also a concer n during an outdoor release, especially if exhaust fans are not in continuous operation, due to wind effects and chimney effects (air movement due to differential temperature).	to serve as supply and return headers. The divider is insulated to minimize heat transfer from one side to the other.
6.2	Is roof access limited to authorized personnel by means of locking mechanisms? Is access to mechanical areas similarly controlled?	Roofs are like entrances to the building and are like mechanical rooms when HVAC is installed. Adjacent structures or landscaping should not allow access to the roof. References: *GSA PBS-P100, CDC/NIOSH Pub 2002-139*, and *LBNL Pub 51959*	Unknown without a more detailed on-site assessment.
6.3	Are there multiple air intake locations?	Single air intakes may feed several air handling units. Indicate if the air intakes are localized or separated. Installing low-leakage dampers is one way to provide the system separation when necessary. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	No.
6.4	What are the types of air filtration? Include the efficiency and number of filter modules for each of the main air handling systems. Is there any collective	MERV – Minimum Efficiency Reporting Value HEPA – High Efficiency Particulate Air Activated charcoal for gases Ultraviolet C for biologicals Consider mix of approaches for optimum protection and cost-effectiveness. Reference: *CDC/NIOSH Pub*	Standard industrial grade filters are used.

	protection for chemical, biological, and radiological contamination designed into the building?	*2002-139*	
6.5	Is there space for larger filter assemblies on critical air handling systems?	Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. However, upgraded filtration may have negative effects upon the overall air handling system operation, such as increased pressure drop. Reference: *CDC/NIOSH Pub 2002-139*	Unknown without a more detailed on-site assessment.
6.6	Are there provisions for air monitors or sensors for chemical or biological agents?	Duct mounted sensors are usually found in limited cases in laboratory areas. Sensors generally have a limited spectrum of high reliability and are costly. Many different technologies are undergoing research to provide capability. Reference: *CDC/NIOSH Pub 2002-139*	Unknown without a more detailed on-site assessment.
6.7	By what method are air intakes and exhausts closed when not operational?	Motorized (low-leakage, fast-acting) dampers are the preferred method for closure with fail-safe to the closed position so as to support in-place sheltering. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	Unknown without a more detailed on-site assessment.
6.8	How are air handling systems zoned? What areas and functions do each of the primary air handling systems serve?	Understanding the critical areas of the building that must continue functioning focuses security and hazard mitigation measures. Applying HVAC zones that isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building HVAC zones and maintaining negative pressure within these areas will contain CBR releases. Identify common return systems that service more than one zone, effectively making a large single zone. Conversely, emergency egress routes should receive positive pressurization to ensure	Unknown without a more detailed on-site assessment.

		contamination does not hinder egress. Consider filtering of the pressurization air. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.9	Are there large central air handling units or are there multiple units serving separate zones?	Independent units can continue to operate if damage occurs to limited areas of the building. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	The HVAC ducts are divided in half to allow them to serve as supply and return headers. The divider is insulated to minimize heat transfer from one side to the other.
6.10	Are there any redundancies in the air handling system? Can critical areas be served from other units if a major system is disabled?	Redundancy reduces the security measures required compared to a non-redundant situation. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
6.11	Is the air supply to critical areas compartmentalized? Similarly, are the critical areas or the building as a whole, considered tight with little or no inleakage?	During chemical, biological, and radiological situations, the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects. Smoke testing of the air supply to critical areas may be necessary. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	Unknown without a more detailed on-site assessment.
6.12	Are supply, return, and exhaust air systems for critical areas secure? Are all supply and return ducts completely connected	The air systems to critical areas should be inaccessible to the public, especially if the ductwork runs through the public areas of the building. It is also more secure to have a ducted air handling system versus sharing hallways and plenums above drop	Unknown without a more detailed on-site assessment.

	to their grilles and registers and secure? Is the return air not ducted?	ceilings for return air. Non-ducted systems provide greater opportunity for introducing contaminants. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	
6.13	What is the method of temperature and humidity control? Is it localized or centralized?	Central systems can range from monitoring only to full control. Local control may be available to override central operation. Of greatest concern are systems needed before, during, and after an incident that may be unavailable due to temperature and humidity exceeding operational limits (e.g., main telephone switch room). Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	The main heater sends hot air into the Heating, Ventilation and Air Conditioning (HVAC) Room, next to the M&E Room. From here it is distributed throughout the building. Offices, restrooms and the employee's lounge are directly heated by this warm air. The Computer Center and the Communications Center use Digital Environmental Managers (DEM) to direct the warm air where it is needed, add or remove humidity from the air or even cool some areas while warming others. Cooling (or heat removal) is done by two chillers in the M&E room. Three Trane 100-ton chillers are available; normally only two are needed to cover all heat loads. The chillers remove heat from the Chilled Water System, and use the Condenser Water System to send the waste heat to two rooftop Cooling Towers. The Chilled Water is then routed from the chillers to air

			handlers for the majority of the building; cooling for the Computer Center and the Communications Center is done by directing Chilled Water to the DEMs. Chiller operation along with Chilled Water and Condenser Water flow are managed from a single control unit in the M&E room. A single Chilled Water pump provides adequate flow for all cooling situations; a backup pump is available at the push of a button. The same is true for the Condenser Water pumps.
6.14	Where are the building automation control centers and cabinets located? Are they in secure areas? How is the control wiring routed?	Access to any component of the building automation and control system could compromise the functioning of the system, increasing vulnerability to a hazard or precluding their proper operation during a hazard incident. The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack. References: *FEMA 386-7, DOC CIAO Vulnerability Assessment Framework 1.1 and LBNL Pub 51959*	Unknown without a more detailed on-site assessment.
6.15	Does the control of air handling systems support plans for sheltering in place or other protective approach?	The micro-meteorological effects of buildings and terrain can alter travel and duration of chemical agents and hazardous material releases. Shielding in the form of sheltering in place can protect people and property from harmful effects. To support in-place sheltering, the air handling systems require	Unknown without a more detailed on-site assessment.

		the ability for authorized personnel to rapidly turn off all systems. However, if the system is properly filtered, then keeping the system operating will provide protection as long as the air handling system does not distribute an internal release to other portions of the building. Reference: *CDC/NIOSH Pub 2002-139*	
6.16	Are there any smoke evacuation systems installed? Does it have purge capability?	For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high-risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk on internal events, such as lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants. References: *GSA PBS-P100, CDC/NIOSH Pub 2002-139, and LBNL Pub 51959*	Yes.
6.17	Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)	Roof-mounted equipment should be kept away from the building perimeter. Reference: *U.S. Army TM 5-853*	Unknown without a more detailed on-site assessment.
6.18	Are fire dampers installed at all fire barriers? Are all dampers functional and seal well when closed?	All dampers (fire, smoke, outdoor air, return air, bypass) must be functional for proper protection within the building during an incident. Reference: *CDC/NIOSH Pub 2002-139*	Yes.
6.19	Do fire walls and fire doors maintain their integrity?	The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal, by zone ducting, fire walls, fire stops, and fire doors) provides energy conservation benefits and functional benefits during a CBR incident.	Unknown without a more detailed on-site assessment.

		Reference: *LBNL Pub 51959*	
6.20	Do elevators have recall capability and elevator emergency message capability?	Although a life-safety code and fire response requirement, the control of elevators also has benefit during a CBR incident. The elevators generate a piston effect, causing pressure differentials in the elevator shaft and associated floors that can force contamination to flow up or down. Reference: *LBNL Pub 51959*	No elevators in HIC.
6.21	Is access to building information restricted?	Information on building operations, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel. References: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	No.
6.22	Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure CBR equipment is functional?	Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired. The HVAC system can be operated in different ways, depending upon an external or internal release and where in the building an internal release occurs. Thus maintenance and security staff must have the training to properly operate the HVAC system under different circumstances, even if the procedure is to turn off all air movement equipment. Reference: *CDC/NIOSH Pub 2002-139 and LBNL Pub 51959*	Unknown without a more detailed on-site assessment.

7	**Plumbing and Gas Systems**		
7.1	What is the method of water distribution?	Central shaft locations for piping are more vulnerable than multiple riser locations. Reference: Physical Security Assessment for the Department of Veterans Affairs Facilities	Unknown without a more detailed on-site assessment.
7.2	What is the method of gas distribution? (heating, cooking, medical, process)	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
7.3	Is there redundancy to the main piping distribution?	Looping of piping and use of section valves provide redundancies in the event sections of the system are damaged. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
7.4	What is the method of heating domestic water? What fuel(s) is used?	Single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types. Domestic hot water availability is an operational concern for many building occupancies. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
7.5	Where are gas storage tanks located? (heating, cooking, medical, process) How are they piped to the distribution system? (above or below ground)	The concern is that the tanks and piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher-risk area. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
7.6	Are there reserve supplies of critical gases?	Localized gas cylinders could be available in the event of damage to the central tank system. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.

8	**Electrical Systems**		
8.1	Are there any transformers or switchgears located outside the building or accessible from the building exterior? Are they vulnerable to public access? Are they secured?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Transformers providing electricity to this site are located outside the building. The two 12.47KV feeders lead to two separate transformers outside the building, one near the north side, and the other near the south side.
8.2	What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
8.3	How are the electrical rooms secured and where are they located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
8.4	Are critical electrical systems co-located with other building systems? Are critical electrical systems located in areas outside of secured electrical areas? Is security system wiring located separately from electrical and other service systems?	Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Yes.
8.5	How are electrical distribution panels serving branch circuits secured or are they in secure locations?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
8.6	Does emergency backup power exist for all areas within the building or for	There should be no single critical node that allows both the normal electrical service and the	Yes. Critical computer

	critical areas only? How is the emergency power distributed? Is the emergency power system independent from the normal electrical service, particularly in critical areas?	emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear are the initial concerns. Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible. Reference: *GSA PBS-P100*	systems are backed up by an UPS which is maintained separately from the sites generator back-up power.
8.7	How is the primary electrical system wiring distributed? Is it co-located with other major utilities? Is there redundancy of distribution to critical areas?	Central utility shafts may be subject to damage, especially if there is only one for the building. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.

9	**Fire Alarm Systems**		
9.1	Is the building fire alarm system centralized or localized? How are alarms annunciated, both locally and centrally? Are critical documents and control systems located in a secure yet accessible location?	Fire alarm systems must first warn building occupants to evacuate for life safety. Then they must inform the responding agency to dispatch fire equipment and personnel. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Centralized.
9.2	Where are the fire alarm panels located? Do they allow access to unauthorized personnel?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Building next to HIC.
9.3	Is the fire alarm system stand-alone or integrated with other functions such as security and environmental or building management systems?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Standalone.

	What is the interface?		
9.4	Do key fire alarm system components have fire- and blast-resistant separation?	This is especially necessary for the fire command center or fire alarm control center. The concern is to similarly protect critical components as described in Items 2.19, 5.7, and 10.3.	Unknown without a more detailed on-site assessment.
9.5	Is there redundant off-premises fire alarm reporting?	Fire alarms can ring at a fire station, at an intermediary alarm monitoring center, or autodial someone else. See Items 5.21 and 10.5.	Yes.

10	**Communications and IT Systems**		
10.1	Where is the main telephone distribution room and where is it in relation to higher risk areas? Is the main telephone distribution room secure?	One can expect to find voice, data, signal, and alarm systems to be routed through the main telephone distribution room. Reference: *FEMA 386-7*	Communications.
10.2	Does the telephone system have an UPS (uninterruptible power supply)? What is its type, power rating, operational duration under load, and location? (battery, on-line, filtered)	Many telephone systems are now computerized and need a UPS to ensure reliability during power fluctuations. The UPS is also needed to await any emergency power coming on line or allow orderly shutdown. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Unknown without a more detailed on-site assessment.
10.3	Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they co-located with other utilities? Are they in secure areas?	Concern is to have separation distance from other utilities and higher-risk areas to avoid collateral damage. Security approaches on the closets include door alarms, closed circuit television, swipe cards, or other logging notifications to ensure only authorized personnel have access to these closets. Reference: *FEMA 386-7*	Unknown without a more detailed on-site assessment.
10.4	How is communications system wiring distributed? (secure chases and risers, accessible public areas)	The intent is to prevent tampering with the systems. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.

10.5	Are there redundant communications systems available?	Critical areas should be supplied with multiple or redundant means of communications. Power outage phones can provide redundancy as they connect directly to the local commercial telephone switch off site and not through the building telephone switch in the main telephone distribution room. A base radio communication system with antenna can be installed in stairwells, and portable sets distributed to floors. References: *GSA PBS-P100 and FEMA 386-7*	No.
10.6	Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure? Where are the secondary and/or intermediate distribution facilities and are they secure?	Concern is collateral damage from manmade hazards and redundancy of critical functions. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Interior and secure.
10.7	What type and where are the WAN (wide area network) connections?	Critical facilities should have two Minimum-Points-of-Presence (MPOPs) where the telephone company's outside cable terminates inside the building. It is functionally a service entrance connection that demarcates where the telephone company's property stops and the building owner's property begins. The MPOPs should not be collocated and they should connect to different telephone company central offices so that the loss of one cable or central office does not reduce capability. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
10.8	What type, power rating, and location of the UPS (uninterruptible power supply)? (battery, on-line, filtered)	Consider that UPS should be found at all computerized points from the main distribution facility to individual data closets and at critical personal computers/terminals.	Lead acid battery.

	Are the UPS also connected to emergency power?	Critical LAN sections should also be on backup power. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	
10.9	What type of LAN (local area network) cabling and physical topology is used? (Category(Cat) 5, Gigabit Ethernet, Ethernet, Token Ring)	The physical topology of a network is the way in which the cables and computers are connected to each other. The main types of physical topologies are: Bus (single radial where any damage on the bus affects the whole system, but especially all portions downstream) Star (several computes are connected to a hub and many hubs can be in the network – the hubs can be critical nodes, but the other hubs continue to function if one fails) Ring (a bus with a continuous connection - least used, but can tolerate some damage because if the ring fails at a single point it can be rerouted much like a looped electric or water system) The configuration and the availability of surplus cable or spare capacity on individual cables can reduce vulnerability to hazard incidents. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
10.10	For installed radio/wireless systems, what are their types and where are they located? (RF (radio frequency), HF (high frequency), VHF (very high frequency), MW (medium wave)	Depending upon the function of the wireless system, it could be susceptible to accidental or intended jamming or collateral damage. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
10.11	Do the IT (Information Technology – computer) systems meet requirements of confidentiality, integrity, and availability?	Ensure access to terminals and equipment for authorized personnel only and ensure system up-time to meet operational needs. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Yes.

10.12	Where is the disaster recovery/mirroring site?	A site with suitable equipment that allows continuation of operations or that mirrors (operates in parallel to) the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	In local geographic area.
10.13	Where is the back-up tape/file storage site and what is the type of safe environment? (safe, vault, underground) Is there redundant refrigeration in the site?	If equipment is lost, data are most likely lost, too. Backups are needed to continue operations at the disaster recovery site or when equipment can be delivered and installed. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Unknown without a more detailed on-site assessment.
10.14	Are there any SATCOM (satellite communications) links? (location, power, UPS, emergency power, spare capacity/capability)	SATCOM links can serve as redundant communications for voice and data if configured to support required capability after a hazard incident. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Unknown without a more detailed on-site assessment.
10.15	Is there a mass notification system that reaches all building occupants? (public address, pager, cell phone, computer override, etc.) Will one or more of these systems be operational under hazard conditions? (UPS, emergency power)	Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident if there is redundancy and power. Reference: *DoD UFC 4-010-01*	No.
10.16	Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass	Reference: *GSA PBS-P100*	Yes, large conference room.

	notification, etc.? (emergency operations, security, fire alarms, building automation) Do the alternate locations also have access to backup systems, including emergency power?		

11	**Equipment Operations and Maintenance**		
11.1	Are there composite drawings indicating location and capacities of major systems and are they current? (electrical, mechanical, and fire protection; and date of last update) Do updated O&M (operation and maintenance) manuals exist?	Within critical infrastructure protection at the building level, the current configuration and capacity of all critical systems must be understood to ensure they meet emergency needs. Manuals must also be current to ensure operations and maintenance keeps these systems properly functioning. The system must function during an emergency unless directly affected by the hazard incident. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
11.2	Have critical air systems been rebalanced? If so, when and how often?	Although the system may function, it must be tested periodically to ensure it is performing as designed. Balancing is also critical after initial construction to set equipment to proper performance per the design. Rebalancing may only occur during renovation. Reference: *CDC/NIOSH Pub 2002-139*	Unknown without a more detailed on-site assessment.
11.3	Is air pressurization monitored regularly?	Some areas require positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation. Measuring pressure drop across filters is an indication when filters should be changed, but also may indicate that low pressures are developing downstream and could result in loss of expected	Unknown without a more detailed on-site assessment.

		protection. Reference: *CDC/NIOSH Pub 2002-139*	
11.4	Does the building have a policy or procedure for periodic recommissioning of major M/E/P (Mechanical/Electrical/ Plumbing) systems?	Recommissioning involves testing and balancing of systems to ascertain their capability to perform as described. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
11.5	Is there an adequate operations and maintenance program including training of facilities management staff?	If O&M of critical systems is done with in-house personnel, management must know what needs to be done and the workforce must have the necessary training to ensure systems reliability. Reference: *CDC/NIOSH Pub 2002-139*	Unknown without a more detailed on-site assessment.
11.6	What maintenance and service agreements exist for M/E/P systems?	When an in-house facility maintenance work force does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as if the work was being done by in-house personnel. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
11.7	Are backup power systems periodically tested under load?	Loading should be at or above maximum connected load to ensure available capacity and automatic sensors should be tested at least once per year. Periodically (once a year as a minimum) check the duration of capacity of backup systems by running them for the expected emergency duration or estimating operational duration through fuel consumption, water consumption, or voltage loss. Reference: *FEMA 386-7*	Unknown without a more detailed on-site assessment.

11.8	Is stairway and exit sign lighting operational?	The maintenance program for stairway and exit sign lighting (all egress lighting) should ensure functioning under normal and emergency power conditions. Expect building codes to be updated as emergency egress lighting is moved from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured. Reference: *FEMA 386-7*	Yes.

13	**Security Master Plan**		
13.1	Does a written security plan exist for this site or building? When was the initial security plan written and last revised? Who is responsible for preparing and reviewing the security plan?	The development and implementation of a security master plan provides a roadmap that outlines the strategic direction and vision, operational, managerial, and technological mission, goals, and objectives of the organization’s security program. Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	HIC does have a fire evacuation plan. HIC does not have a mass evacuation plan and rally point.
13.2	Has the security plan been communicated and disseminated to key management personnel and departments?	The security plan should be part of the building design so that the construction or renovation of the structure integrates with the security procedures to be used during daily operations. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.3	Has the security plan been benchmarked or compared against related organizations and operational entities?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.4	Has the security plan ever been tested and evaluated from a cost-benefit and operational efficiency and effectiveness perspective?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.

13.5	Does it define mission, vision, short-long term security program goals and objectives?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.6	Are threats, vulnerabilities, risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Unknown without a more detailed on-site assessment.
13.7	Has a security implementation schedule been established to address recommended security solutions?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.8	Have security operating and capital budgets been addressed, approved and established to support the plan?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.9	What regulatory or industry guidelines/standards were followed in the preparation of the security plan?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.10	Does the security plan address existing security conditions from an administrative, operational, managerial and technical security systems perspective?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.11	Does the security plan address the protection of people, property, assets, and information?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.12	Does the security plan address the following major components: access control, surveillance, response, building hardening and protection against biological, chemical, radiological and cyber-network attacks?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.

13.13	Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
13.14	When was the last security assessment performed? Who performed the security risk assessment?	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	Unknown without a more detailed on-site assessment.
13.15	Were the following areas of security analysis addressed in the security master plan: Asset Analysis: Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current value, and replacement value? Threat Analysis: Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? (possible criminal acts (documented and review of police/security incident reports) associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings) Vulnerability Analysis: Does the security plan address other areas and	This process is the input to the building design and what mitigation measures will be included in the facility project to reduce risk and increase safety of the building and people. Reference: *USA TM 5-853, Security Engineering*	Unknown without a more detailed on-site assessment.

	anything else associated with a site or building and it's operations that can be taken advantage of to carry out a threat? (architectural design and construction of new and existing buildings, technological support systems (e.g. heating, air conditioning, power, lighting and security systems, etc.) and operational procedures, policies and controls) Risk Analysis: Does the security plan address the findings from the asset, threat, and vulnerability analyses to develop, recommend and consider implementation of appropriate security countermeasures?		

Building Design Mitigation Measures

Asset-Threat/Hazard Pair	Current Risk Rating	Suggested Mitigation Measure	Revised Risk Rating
1. Explosive Blast/Structural	High	FRF film on window	Medium
2. Explosive Blast/Structural	High	Enclose open entrance area	Medium
3. Chemical/Mechanical	High	Extend Air Intake	Medium
4. Biological/Mechanical	High	Extend Air Intake	Medium
5. Radiological/Site	Medium	Mass Evacuation Plan and Rally Point	Low

Unit X

COURSE TITLE Building Design for Homeland Security

TIME 45 minutes

UNIT TITLE Electronic Security Systems

OBJECTIVES

1. Use the assessment process to identify electronic security system requirements that are needed to mitigate vulnerabilities
2. Describe the electronic security system concepts and practices that warrant special attention to enhance public safety
3. Explain the basic concepts of electronic security system components, their capabilities, and their interaction with other systems
4. Justify selection of electronic security systems to mitigate vulnerabilities

SCOPE

The following topics will be covered in this unit:

1. Control centers and building management systems
2. Perimeter layout and zoning of sensors
3. Intrusion detection systems and sensor technologies
4. Entry-control systems and electronic entry control technologies
5. Closed circuit television and data-transmission media
6. Definitions of the degree of security and control

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 3-47 to 3-50; Appendix D; and Security Systems and Security Master Plan sections of Checklist at end of Chapter (pages 1-81 – 1-92)
2. Unit X visuals
3. Case Study

REQUIREMENTS

1. Overhead projector or computer display unit
2. Unit X visuals
3. Instructor Guide
4. Student Manual

UNIT X OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

  The Instructor will walk the students through the various components and technology currently available for use in security systems, including biometrics for access control, closed circuit television, and terminology to describe levels of security. These are the mitigation measures available to reduce risks due to vulnerabilities in physical security systems.

- **Optional Activity:** There are no optional activities in this Unit.

- **Activity:** There is no student activity associated with this Unit. However, any mitigation measures identified as a priority to reduce high risks will be covered in Unit XI as part of the group presentation.

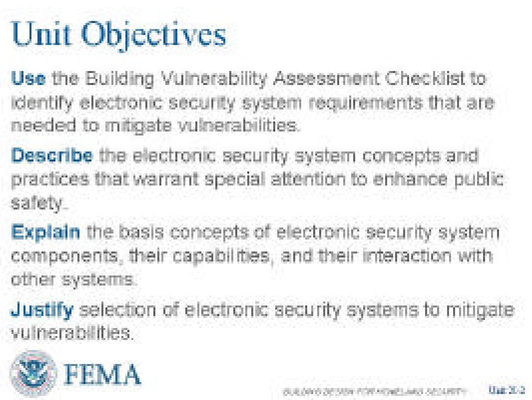
INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL X-1

Introduction and Unit Overview

This is Unit X Electronic Security Systems (ESS). This unit will describe the types of sensors, concepts of operation of electronic security systems, and terminology used in the industry.

VISUAL X-2



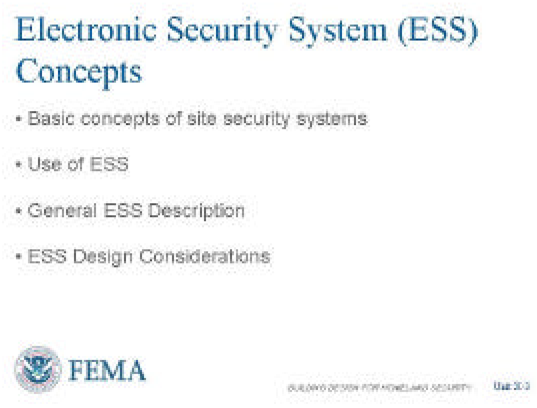
Unit Objectives

At the end of this unit, you should be able to:

1. Use the Building Vulnerability Assessment Checklist to identify electronic security system requirements that are needed to mitigate vulnerabilities.
2. Describe the electronic security system concepts and practices that warrant special attention to enhance public safety.
3. Explain the basis concepts of electronic security system components, their capabilities, and their interaction with other systems.
4. Justify selection of electronic security systems to mitigate vulnerabilities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL X-3



Electronic Security Systems Concepts

The **Building Vulnerability Assessment Checklist**, **Section 12,** can be used for the assessment of security systems. Security systems historically have been designed, installed, serviced, and monitored by physical security companies, typically after the completion of the building. New Internet and wireless technologies have significantly changed the way in which security systems are designed and now incorporation of security system design and processes should begin at the earliest stages of design or renovation. An electronic security system is the physical implementation of the elements of the Layers of Defense:

- Deter
- Detect
- Deny
- Devalue

In this unit, the student should have an appreciation for:

- Basic concepts of ESS
- Use of ESS
- General ESS Description
- ESS Design Considerations

Fundamental objective:

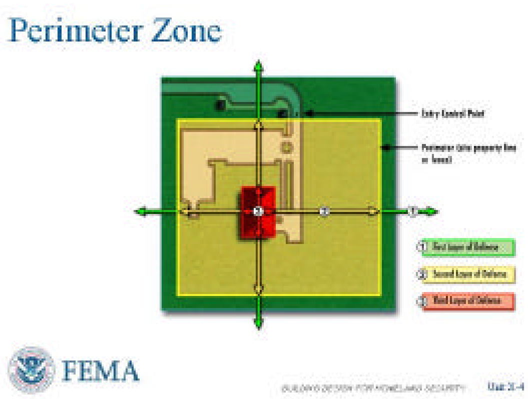
Provide appropriate, effective, and economical protective design for assets.

Approach:

Coordinated effort between security and law enforcement and engineering communities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL X-4



Perimeter Zone

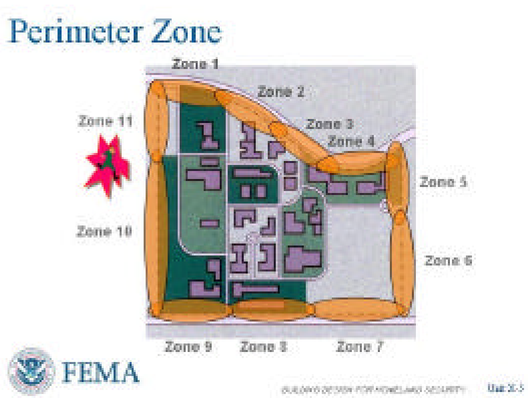
The protection of a facility is designed with layers of defense, detection, and response. Before we discuss security systems, we need to review several basic concepts:

- A protected area's perimeter is usually defined by an enclosing wall or fence or a natural barrier such as water. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined.

Perimeter Zone and Layers of Defense

- First layer of defense is from the perimeter outward.
- Second layer of defense is between the building and the perimeter.
- Third layer of defense is inside the building.

VISUAL X-5



Perimeter Layout and Zoning Sensors

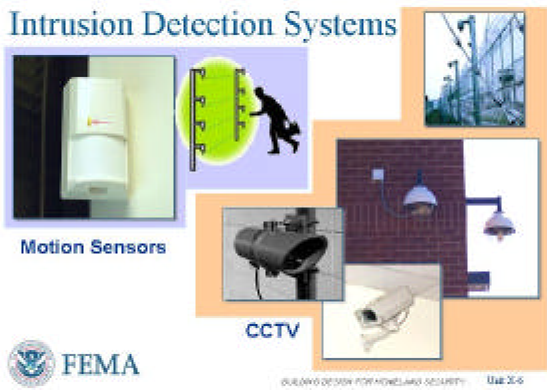
- After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, the existing terrain, and the operational activities along the perimeter.
- The exterior and interior Intrusion and Detection Systems should be configured as layers of unbroken rings concentrically surrounding the asset. These rings should correspond to defensive layers that constitute the delay system. The first detection layer is located at the outermost defensive layer necessary to provide the required delay. Detection layers can be on a defensive layer, in the area between two defensive layers, or on the asset itself,

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

depending on the delay required.

- If an alarm occurs in a specific zone, the operator can readily determine its approximate location by referring to a map of the perimeter.

VISUAL X-6

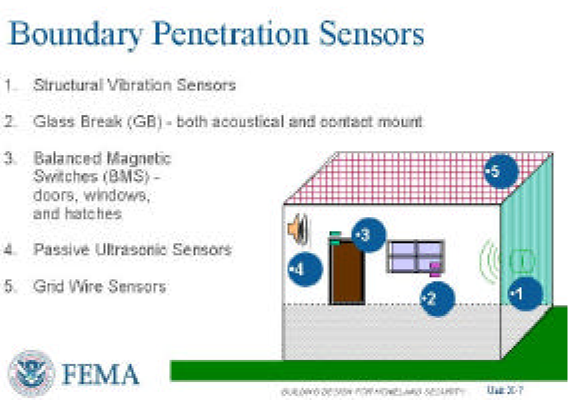


Intrusion Detection Systems

There are a number of different sensor technologies:

- Boundary Penetration Sensors
- Volumetric Motion Sensors
- Exterior Intrusion Detection Sensors
- Fence Sensors
- Buried Line Sensors
- Microwave Sensors
- Infrared Sensors
- Video Motion Sensors

VISUAL X-7



Boundary Penetration Sensors

- Structural Vibration Sensors
- Glass Breaking Sensors
- Balanced Magnetic Switches
- Passive Ultrasonic Sensors
- Grid Wire Sensors

Structural vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives, or employing other forcible methods of entry.

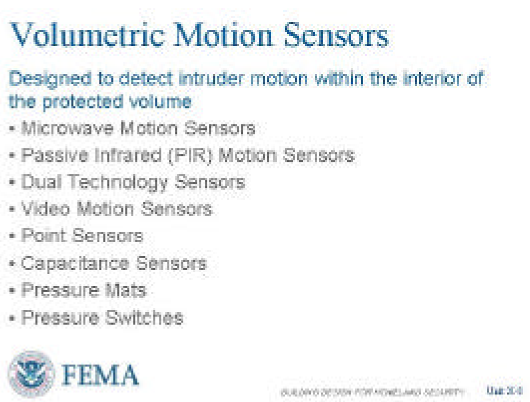
Glass breaking sensors detect the breaking of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range.

Balanced magnetic switches (BMSs) are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry.

Passive ultrasonic sensors detect acoustical energy in the ultrasonic frequency range, typically between 20 and 30 kilohertz (kHz). They are used to detect an attempted penetration through rigid barriers (such as metal or masonry walls, ceilings, and floors). and windows and vents covered by metal grilles, shutters, or bars if these openings are properly sealed against outside sounds.

Grid wire sensors consist of a continuous electrical wire arranged in a grid pattern. The wire maintains an electrical current. An alarm is generated when the wire is broken. The sensor detects forced entry through walls, floors, ceilings, doors, windows, and other barriers.

VISUAL X-8



Volumetric Motion Sensors

Designed to detect intruder motion within the interior of the protected volume

- Microwave Motion Sensors
- Passive Infrared (PIR) Motion Sensors
- Dual Technology Sensors
- Video Motion Sensors
- Point Sensors
- Capacitance Sensors
- Pressure Mats
- Pressure Switches

Microwave motion sensors use high-frequency electromagnetic energy to detect an intruder's motion within the protected area. Interior or sophisticated microwave motion sensors are normally used.

Interior microwave motion sensors are typically monostatic; the transmitter and the receiver are housed in the same enclosure (transceiver).

Sophisticated microwave motion sensors may be equipped with electronic range gating. This feature allows the sensor to ignore the signals reflected beyond the settable detection range. Range gating may be used to effectively minimize unwanted alarms from activity outside the protected area.

Passive infrared (PIR) motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.

Dual technology sensors combine two different technologies in one unit to minimize the generation of alarms caused by sources other than intruders.

Video motion sensors generate an alarm when an intruder enters a selected portion of a CCTV camera's field of view. The sensor processes and compares successive images between the images against predefined alarm criteria. There are two categories of video motion detectors, analog and digital. Analog detectors generate an alarm in response to changes in a picture's contrast. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image.

Point sensors are used to protect specific objects within a facility. These sensors (sometimes referred to as proximity sensors)

INSTRUCTOR NOTES	CONTENT/ACTIVITY

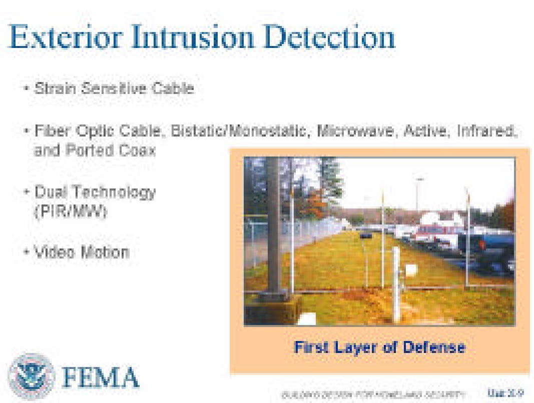
detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches.

Capacitance sensors detect an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground.

Pressure mats generate an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat.

Pressure switches are mechanically activated contact switches or single ribbon switches.

VISUAL X-9



Exterior Intrusion Detection Sensors

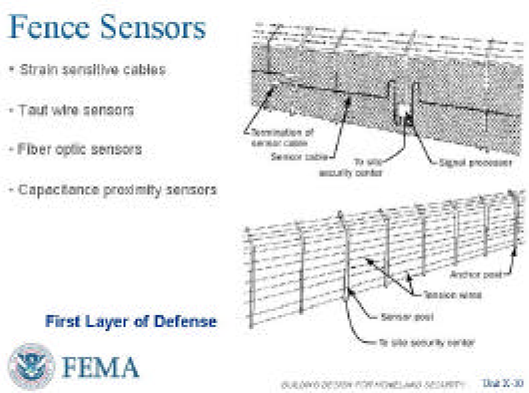
- Strain Sensitive Cable - fences and gates
- Fiber Optic Cable - fences, gates, and gravel pathways
- Bistatic/Monostatic Microwave - line of sight, clear zones
- Active Infrared - portals, short perimeter gap filters
- Ported Coax - exterior clear zones
- Dual Technology (PIR/MW) - portals and gap fillers
- Video Motion - volumetric traffic, open areas

Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones between fences or around buildings, for protecting materials and equipment stored outdoors within a protected boundary, or in estimating the POD for buildings and other facilities.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

Because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms than interior sensors. Inclement weather conditions (e.g., heavy rain, hail, and high wind), vegetation, the natural variation of the temperature of objects in the detection zone, blowing debris, and animals are major sources of unwanted alarms.

VISUAL X-10



Fence Sensors

- Strain sensitive cables
- Taut wire sensors
- Fiber optic sensors
- Capacitance proximity sensors

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts (e.g., climbing, cutting, or lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain.

Strain sensitive cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical distortions or stress resulting from fence motion.

Taut wire sensors combine a physically taut-wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end.

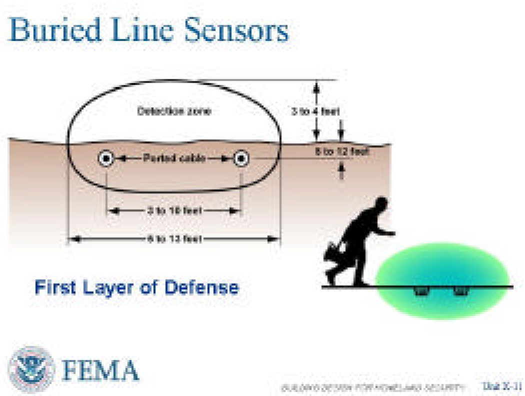
Fiber optic sensors are functionally equivalent to the strain-sensitive cable sensors previously discussed. However, rather than electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed to

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

determine whether an alarm should be initiated.

Capacitance proximity sensors measure the electrical capacitance between the ground and an array of sense wires. Any variations in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm.

VISUAL X-11



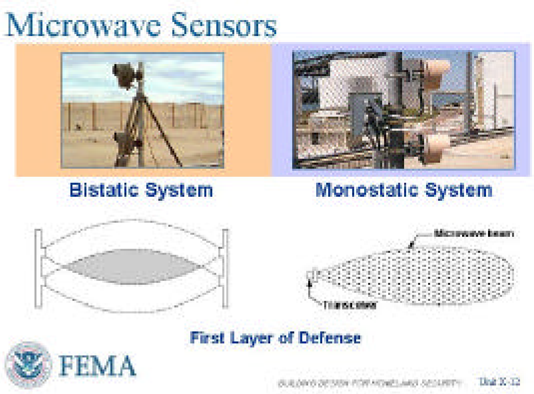
Buried Line Sensors

A buried line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field. Buried line sensors have several significant features:

- They are hidden, making them difficult to detect and circumvent.
- They follow the terrain's natural contour.
- They do not physically interfere with human activity, such as grass mowing or snow removal.
- They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL X-12



Microwave Sensors

- Bistatic system
- Monostatic

Microwave intrusion detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use the same antenna.

A bistatic system uses a transmitter and a receiver that are typically separated by 100 to 1,200 feet and that are within direct line of sight of each other.

Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays for the transmitter and receiver, which are usually combined into a single package.

VISUAL X-13

Infrared (IR) Sensors

The IR sensors are available in both active and passive models. An active sensor generates one or more near-IR beams that generate an alarm when interrupted. A passive sensor detects changes in thermal IR radiation from objects located within its field of view.

Active sensors consist of transmitter/receiver pairs. The transmitter contains an IR light source (such as a gallium arsenide light-emitting diode [LED]) that generates an IR beam. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

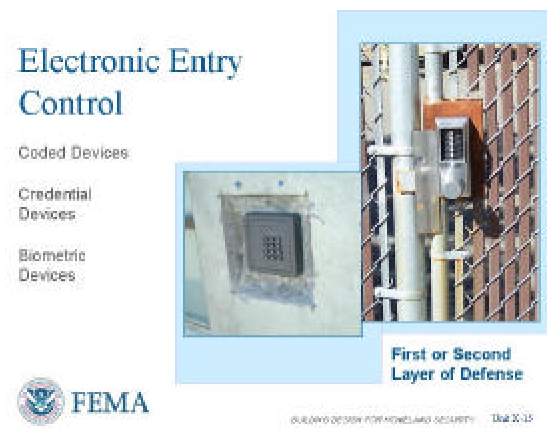
INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

VISUAL X-14

Video Motion Sensors

Video motion sensors are available on most digital video recorders used in security applications. They can be programmed to activate alarms, initiate recording, or any other designated action when motion is detected by a security camera. Some digital video recorders can be programmed to monitor very specific fields of view for specific rates of motion in order to increase effectiveness and minimize extraneous detections. Video motion sensors can also greatly improve the efficiency of security personnel monitoring security cameras by alerting them when motion is detected.

VISUAL X-15



Entry Control Systems and Technology

- Coded Devices
- Credential Devices
- Biometric Devices

The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals. These means of entry control can be applied manually by guards or automatically by using entry control devices. In a manual system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry. In an automated system, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

All entry control systems control passage by using one or more of three basic techniques (e.g., something a person knows, something a person has, or something a person is or does). Automated entry control devices based on these techniques are grouped into three categories: coded, credential, and biometric devices.

VISUAL X-16

Coded Devices

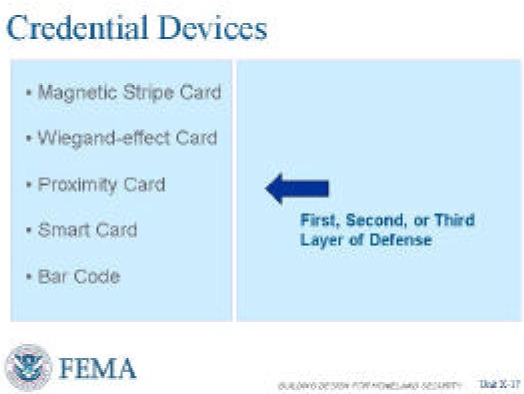
- Electronic Keypad Devices
- Computer Controlled Keypad Devices

Coded devices operate on the principle that a person has been issued a code to enter into an entry control device. This code will match the code stored in the device and permit entry. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Electronically coded devices include electronic and computer controlled keypads.

Electronic keypad devices are similar to telephone keypads (12 keys). This type of keypad consists of simple push-button switches that, when depressed, are decoded by digital logic circuits. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds.

Computer controlled keypad devices are devices similar to electronic keypad devices, except they are equipped with a microprocessor in the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the keys are depressed and may provide additional functions such as personal ID and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

VISUAL X-17



Credential Devices

- Magnetic Stripe Card
- Wiegand-effect Card
- Proximity Card
- Smart Card
- Bar Code

A credential device identifies a person having legitimate authority to enter a controlled area. A coded credential (e.g., plastic card or key) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read.

Magnetic stripe card is a strip of magnetic material located along one edge of the card which is encoded with data (sometimes encrypted). The data is read by moving the card past a magnetic read head.

Wiegand-effect card contains a series of small-diameter, parallel wires approximately ½-inch long, embedded in the bottom half of the card. The wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power.

Proximity card is not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. Several techniques are

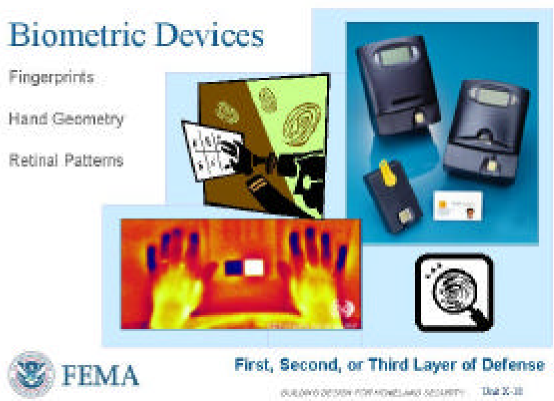
INSTRUCTOR NOTES	CONTENT/ACTIVITY

used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an integrated circuit embedded in the card to generate a code that can be magnetically or electrostatically coupled to the reader.

Smart card is embedded with a microprocessor, memory, communication circuitry, and a battery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry control information and other data may be stored in the microprocessor's memory.

Bar code consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry control applications because it can be easily duplicated.

VISUAL X-18



Biometric Devices

- Fingerprints
- Hand Geometry
- Retinal Patterns

The third basic technique used to control entry is based on the measurement of one or more physical or personal characteristics of an individual. Because most entry control devices based on this technique rely on measurements of biological characteristics, they have become commonly known as biometric devices. Characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood-vessel patterns have been used for controlling entry.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template. If a match is found, entry is granted.

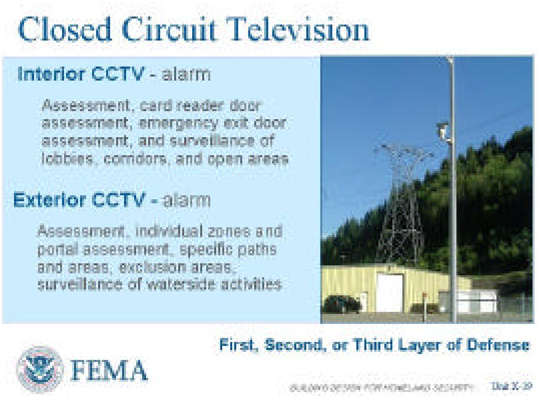
Fingerprints verification devices use one of two approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.

Hand geometry devices use a variety of physical measurements of the hand, such as finger length, finger curvature, hand width, webbing between fingers, and light transmissivity through the skin to verify identity. Both two- and three-dimensional units are available.

Retinal patterns is based on the premise that the pattern of blood vessels on the human eye's retina is unique to an individual. While the eye is focused on a visual target, a low-intensity IR light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood-vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

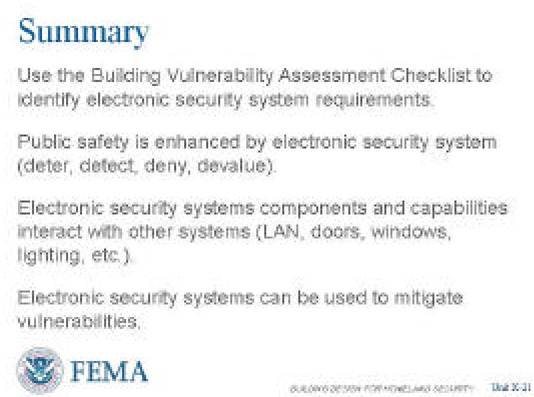
VISUAL X-19



Closed Circuit Television Systems

- Interior CCTV - alarm assessment, card reader door assessment, emergency exit door assessment, and surveillance of lobbies, corridors, and open areas
- Exterior CCTV - alarm assessment, individual zones and portal assessment, specific paths and areas, exclusion areas, surveillance of waterside activities

VISUAL X-20



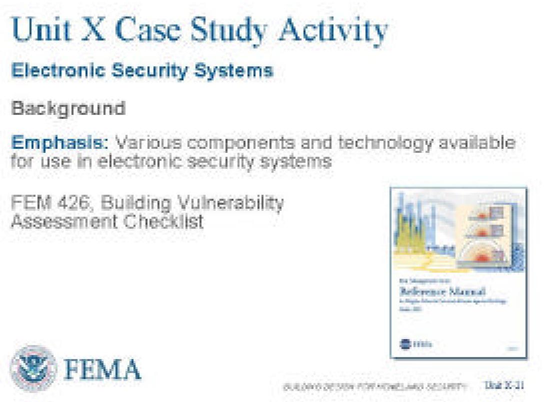
Summary

Remember all the different components of the system must support each others function. For example, the best barriers are those tied to a detection system, like a strain sensitive cable alarm sensor on a chain link fence, with a steel cable woven into the fence, delay function, and overseen by an assessment method, such as a CCTV system.

- Use the Building Vulnerability Assessment Checklist to identify electronic security system requirements.
- Public safety is enhanced by electronic security system (deter, detect, deny, devalue).
- Electronic security systems components and capabilities interact with other systems (LAN, doors, windows, lighting).
- Electronic security systems can be used to mitigate vulnerabilities.

INSTRUCTOR NOTES

VISUAL X-21



Refer participants to FEMA 426, the Unit X Case Study activity in the Student Manual, and the GIS portfolio.

Members of the instructor staff should be available to answer questions and assist groups as needed.

At the end of 10 minutes, reconvene the class and facilitate group reporting.

CONTENT/ACTIVITY

Student Activity

In this Unit, the emphasis will be upon the various components and technology available for use in electronic security systems.

The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment.

Activity Requirements

- Working in small groups, refer to the HIC Case Study and to the GIS portfolio to determine answers to the worksheet questions.
- Then review results to identify vulnerabilities and possible mitigation measures.

Take 10 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

In the next unit, you will finalize and present of Case Study Results. This will include preparation and presentation of the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk. The top three risks will be prioritized as well as the top three recommended mitigation measures with rationale and justification. It includes any consideration for changes to security systems per Unit X.

UNIT X CASE STUDY ACTIVITY:
ELECTRONIC SECURITY SYSTEMS

In this Unit, the emphasis will be upon the various components and technology available for use in electronic security systems. The **Building Vulnerability Assessment Checklist in FEMA 426** can be used as a screening tool for preliminary building design vulnerability assessment.

Requirement

Refer to the HIC Case Study and to the GIS portfolio to determine answers to the questions. Then review results to identify vulnerabilities and possible mitigation measures.

1. Complete the following components of the Building Vulnerability Assessment Checklist that address security systems

2. Upon completion of these portions of the checklist, refer back to the risk ratings determined in Unit VI Case Study Activity and, based on this detailed analysis, decide if the rating is accurate.

3. Select mitigation measures to reduce vulnerability and associated risk from security system design.

4. Estimate the new risk ratings for high risk asset-threat pairs based on the recommended mitigation measures.

Section	Vulnerability Questions	Guidance	Observations
12.1	Are black/white or color CCTV (closed circuit television) cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom? Are they analog or digital by design? What are the number of fixed, wireless and pan-tilt-zoom cameras used? Who are the manufacturers of the CCTV cameras?	Security technology is frequently considered to complement or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost-effective and efficiency perspective. During and after an incident, the system, or its backups, should be	CCTV systems are used in the back parking area, including the loading dock area. The HIC security officer monitors the cameras from his desk. There is a VHS recorder. It is an older generation analog system. Unknown without a more detailed on-site assessment.

	What is the age of the CCTV cameras in use?	functional per the planned design. Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. Reference: *GSA PBS P-100*	
12.2	Are the cameras programmed to respond automatically to perimeter building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
12.3	What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
12.4	Are panic/duress alarm buttons or sensors used, where are they located, and are they hardwired or portable?	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other high risk locations by assessment. Reference: *GSA PBS P-100*	Unknown without a more detailed on-site assessment.
12.5	Are intercom call boxes used in parking areas or along the building perimeter?	See item 12.4.	No.
12.6	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Telephone wire.
12.7	Who monitors the CCTV system?	Reference: *DOC CIAO Vulnerability Assessment Framework 1.1*	The HIC security officer.

12.8	What is the quality of video images both during the day and hours of darkness? Are infrared camera illuminators used?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
12.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.
12.10	What type of exterior Intrusion Detection System (IDS) sensors are used? (electromagnetic; fiber optic; active infrared; bistatic microwave; seismic; photoelectric; ground; fence; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches)	Consider balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors, and review roof intrusion detection. Consider glass break sensors for windows up to scalable heights. Reference: *GSA PBS-P100*	Unknown without a more detailed on-site assessment.
12.11	Is a global positioning satellite system (GPS) used to monitor vehicles and asset movements?	Reference: *Physical Security Assessment for the Department of Veterans Affairs Facilities*	Unknown without a more detailed on-site assessment.

Security System Mitigation Measures

Asset-Threat/Hazard Pair	Current Risk Rating	Suggested Mitigation Measure	Revised Risk Rating
1. Explosive Blast/Site	High	Upgrade CCTVs to digital and use DVRs. Install CCTVs to monitor front parking.	Medium
2. Explosive Blast/Building	High	Upgrade CCTVs to digital and use DVRs. Install CCTVs to monitor interior lobby and loading dock.	Medium
3. Chemical/Mechanical Systems	High	Install basic chemical sensors on outside air intake-HVAC system.	Medium
4. Biological/Mechanical Systems	High	Evaluate acquisition of portable or basic level biological sensors	High to Medium
5. Radiological	High	Evaluate acquisition of portable or basic level radiological sensors	High to Medium

Unit XI

COURSE TITLE	Building Design for Homeland Security **TIME** 135 minutes
UNIT TITLE	Case Study
OBJECTIVES	1. Explain building security design issues to a building owner for consideration prior to a renovation or new construction 2. Explain the identification process to arrive at the high risk asset – threat/hazard pairs 3. Justify the recommended mitigation measures, explaining the benefits in reducing the risk for the high risk situations of interest
SCOPE	The following topics will be covered in this unit: 1. Activity: Preparation and presentation of the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk. The top three risks will be prioritized as well as the top three recommended mitigation measures with rationale and justification. Includes any consideration for changes to security systems per Unit X.
REFERENCES	1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* 2. Student Manual, Unit XI (handouts will be a 1-page summary of analysis results and briefing format for presentation of information) 3. Unit XI visuals 4. Case Study – Hazardville Information Company
REQUIREMENTS	1. Overhead projector or computer display unit 2. Unit XI visuals 3. Instructor Guide 4. Student Manual

UNIT XI OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

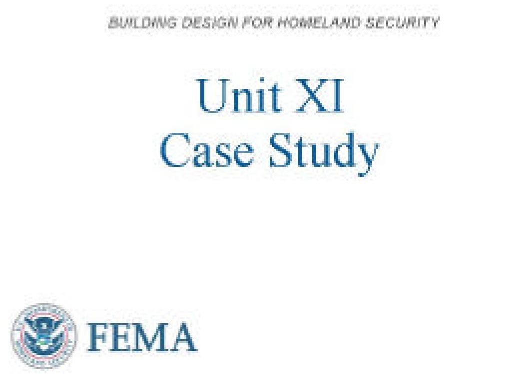
  The Instructor will review the Hazardville Information Inc. site and building portfolio, DoD Antiterrorism Standards, and GSA Interagency Security Criteria, and provide the building owners parameters for the Design Basis Threat and Levels of Protection.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will prepare and present the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk. The top three risks will be prioritized as well as the top three recommended mitigation measures with rationale and justification. Includes any consideration for changes to security systems per Unit X.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-1



Introduction and Unit Overview

This is Unit XI Case Study activity. This unit will review the Hazardville Information Company, Inc., site and building portfolio, DoD Antiterrorism Standards and GSA Interagency Security Criteria, and provide the building owners parameters for the Design Basis Threat and Levels of Protection.

Students will prepare and present the top three risks identified by the group, the vulnerabilities identified for these risks, and top three recommended mitigation measures to reduce vulnerability and risk. The top three risks will be prioritized as well as the top three recommended mitigation measures with rationale and justification. Includes any consideration for changes to security systems per Unit X.

VISUAL XI-2

Unit Objectives

At the end of this unit, you should be able to:

1. Explain building security design issues to a building owner for consideration prior to a renovation or new construction.

2. Explain the identification process to arrive at the high risk asset – threat/hazard pairs.

3. Justify the recommended mitigation measures, explaining the benefits in reducing the risk for the high risk situations of interest.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-3

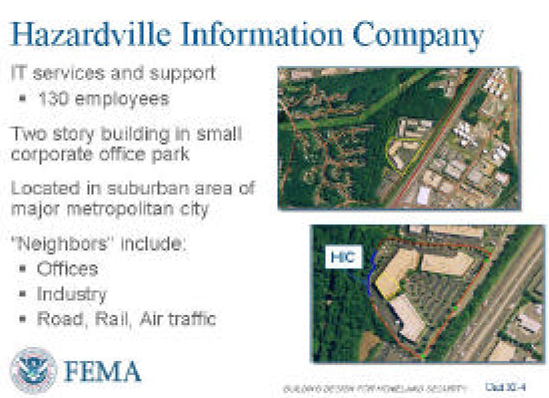
Hazardville Information Company

The Case Study will be a comprehensive review and practical application of FEMA 426.

In this unit, the following topics will be presented:

- Company Functions
- Company Infrastructure
- Threats/Hazards
- Vulnerabilities

VISUAL XI-4



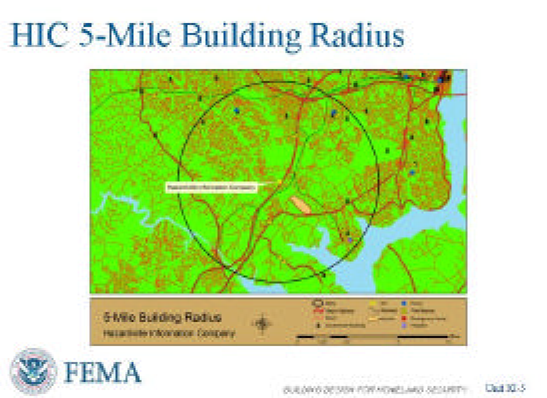
Hazardville Information Company

The Hazardville Information Company supports approximately 1,000 users and 100 applications as a primary data center and as a disaster recovery backup site.

HIC has over 130 employees and approximately 80 to 100 employees are in the building at any given time.

- Regional computer center
- Suburban business park
- Customers and neighbors

VISUAL XI-5

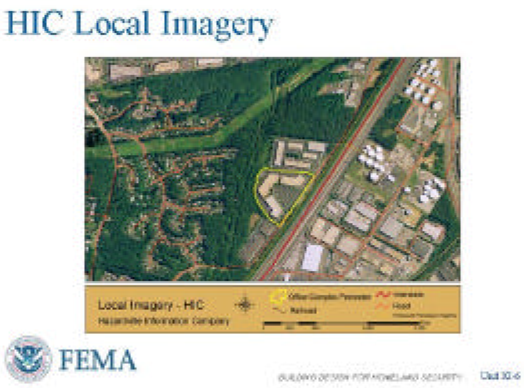


HIC 5-Mile Radius

The Hazardville Information Company is located approximately 15 miles outside of a major urban city in the suburbs, and adjacent to a major interstate highway. There are several commercial iconic properties, one military installation, and several government offices within a 5-mile radius of the HIC building.

INSTRUCTOR NOTES

VISUAL XI-6



CONTENT/ACTIVITY

HIC Local Imagery

The office building is part of a corporate business park. HIC does not control the front parking area, signage, or other general site conditions such as stormwater drainage, lighting, or vehicle and pedestrian traffic flow and movement. The business park is responsible for grounds maintenance to include cutting the grass, planting flowers, trimming trees, sweeping the parking lot, and towing unauthorized vehicles. Trash service is the responsibility of tenants. HIC has a large dumpster located at the rear of the loading dock area approximately 50 feet from the building.

HIC receives the mail and packages at the front office lobby desk. Large packages and equipment are delivered to the rear loading dock. HIC does not have a separate mail room, but does have an internal administrative space with copiers, printers, supplies, and staff mailboxes. The front desk receptionist is responsible for sorting and screening all mail.

The business park is adjacent to a major interstate highway and there are a number of storage tanks, manufacturing and production facilities, and other commercial properties across the interstate.

INSTRUCTOR NOTES	**CONTENT/ACTIVITY**

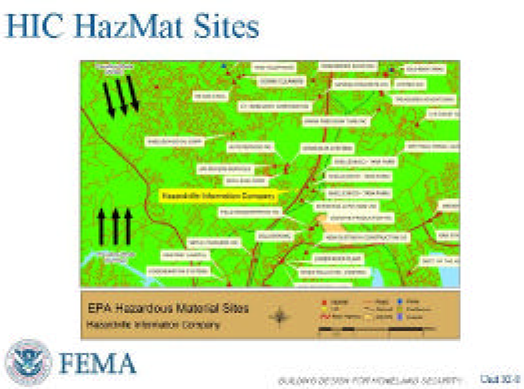
VISUAL XI-7

HIC Office Building

The HIC office space has client and staff parking in the front and a rear parking and loading dock area for supply trucks, vendors, and trash.

The front parking are is unrestricted, but the back parking area is fully enclosed with chain link fencing on the perimeter of the property. There is no gate or means to prevent vehicles from transiting around the rear of the business park.

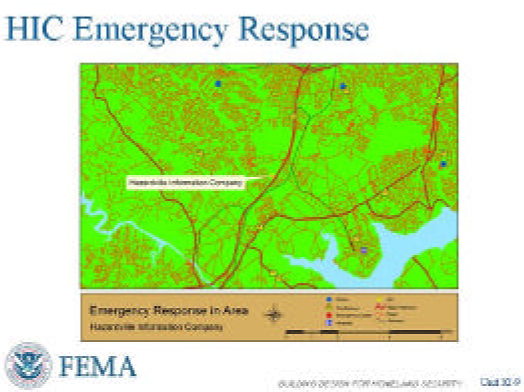
VISUAL XI-8



HIC HazMat Sites

There are a significant number of hazardous waste sites in near proximity to the HIC building. The vast majority are small generators such as gas stations, dry cleaning, and other commercial businesses. Large generators include the petroleum storage and production facility located across the interstate.

VISUAL XI-9

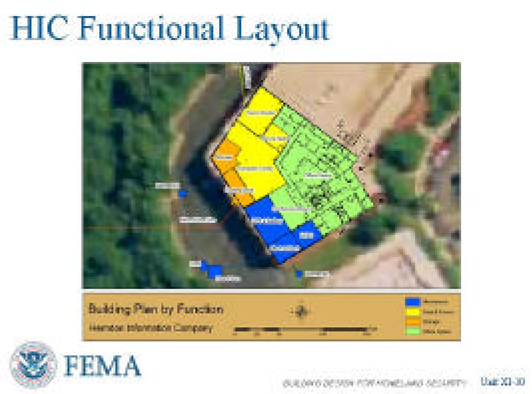


HIC Emergency Response

The local emergency response capabilities include primary police, fire, and medical facilities approximately 8 to 10 miles away. There are multiple means of ingress and egress to the HIC building complex and the site is served by fire mains with a hydrant located approximately 200 feet from the HIC office.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-10



HIC Functional Layout

- Downstairs: Computers Center, Communications, Staff
- Upstairs: Executive offices
- Highbay loading dock, mechanical and electrical (M&E) room

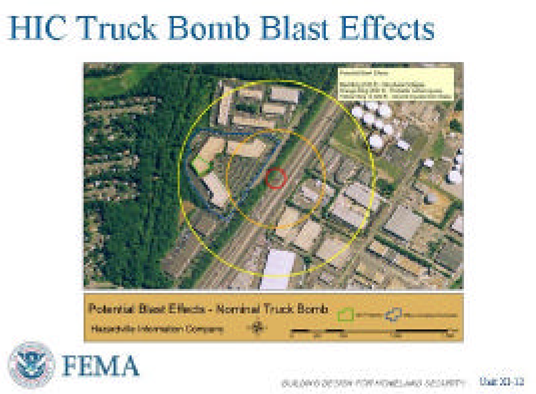
VISUAL XI-11

HIC Car Bomb Blast Effects

The nominal range-to-effects chart radius of influence of a small car bomb detonation at the front entrance indicates that the building would experience significant damage, but likely not suffer progressive collapse. The front façade of the building is approximately 75 percent annealed glass and has an 8-foot overhang. The terrain slopes upward from the parking lot to the main entrance, and is landscaped with flower beds and trees. Key staff would probably be killed and administrative functions destroyed, but the Computer Center and Communications functions would likely survive relatively intact.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

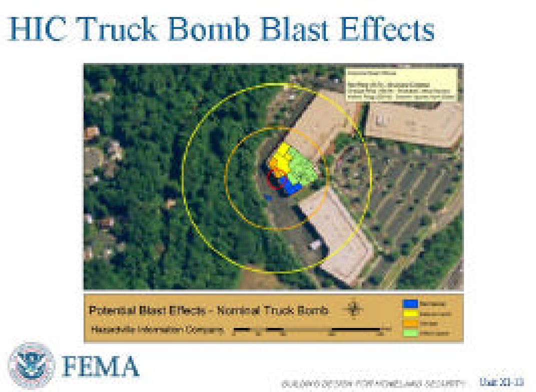
VISUAL XI-12



HIC Truck Bomb Blast Effects

A truck bomb detonation occurring on the interstate would also significantly damage the HIC building, primarily glass breakage and potentially some structural damage. If the truck bomb were to detonate near the tank farm, the ensuing explosion, fire, and plume would have significant impact on the HIC building.

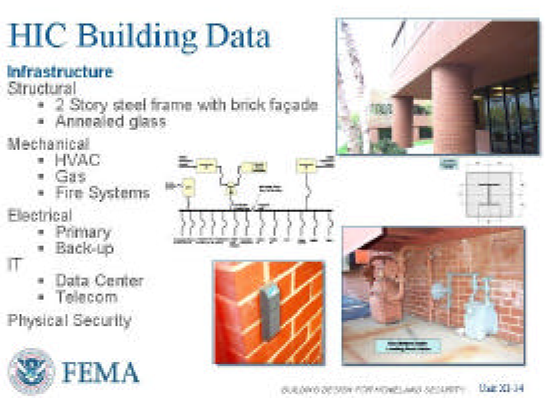
VISUAL XI-13



HIC Truck Bomb Effects

A truck bomb detonation at the rear of the HIC building at the loading dock would result in significant structural damage and potentially progressive collapse. The Computer Center, Communications, and other critical functions would be destroyed. Critical infrastructure that would be destroyed includes the mechanical/electrical room.

VISUAL XI-14



HIC Building Data

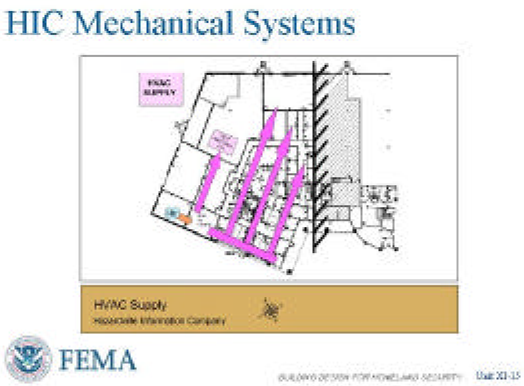
- Structural
- Mechanical
- Electrical
- IT
- Physical Security

HIC Structural System

The HIC building is a two-story steel frame structure with a brick facade and annealed glass.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL XI-15

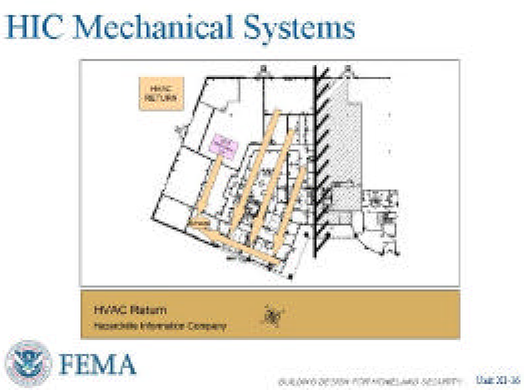


HIC Mechanical Systems

The air used to heat or cool the HIC Headquarters building is filtered in the HVAC room using standard industrial grade MERV 8 filters. Outside make-up air is brought in through a vent in the wall located approximately 3 feet above ground level.

The Computer Data Center has two additional air cooling units located in the data center and uses the main chill water supply. The data center maintains a slight net positive pressure compared to the main office areas.

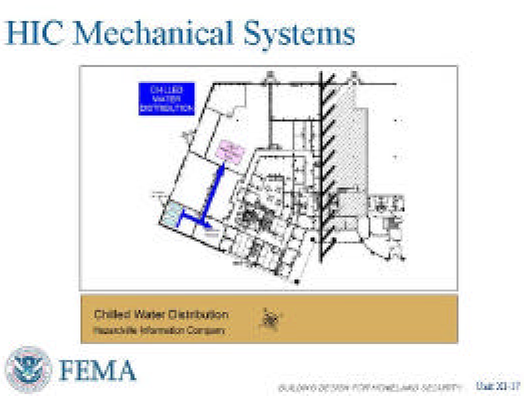
VISUAL XI-16



HIC Mechanical Systems

The return air for the main office space has sufficient room inside the ductwork and mechanical room area to incorporate additional filters and equipment.

VISUAL XI-17

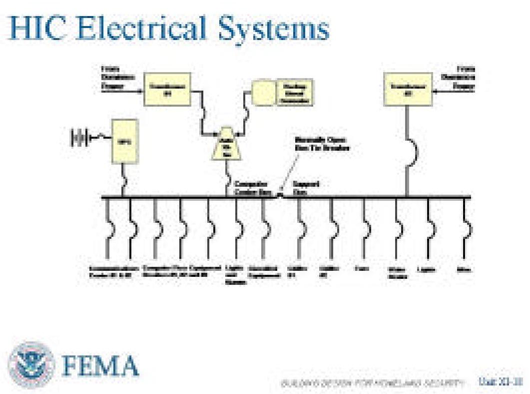


HIC Mechanical Systems

Chiller operation along with chilled water and condenser water flow are managed from a single control unit in the M&E room. A single chilled water pump provides adequate flow for all cooling situations; a backup pump is available at the push of a button. The same is true for the condenser water pumps.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

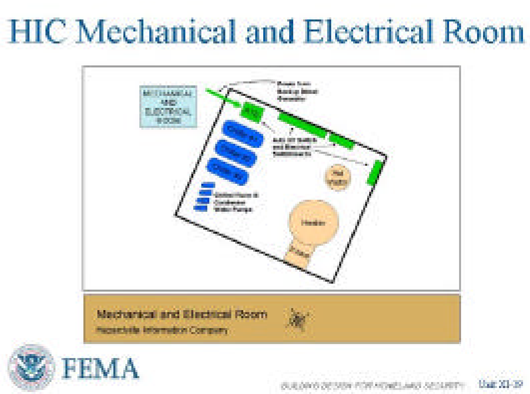
VISUAL XI-18



HIC Electrical One-Line Diagram

HIC's electrical loads are divided between two main electrical buses, the Computer Center Bus (CCB) and the Support Bus (SB). They are located in separate "closets" of the building. A tie breaker allows the buses to be connected, so they can be powered by a single main transformer, or to allow SB loads to be carried by the backup diesel generator. The system is monitored by a digital energy management system, which provides indications, alarms, and instructions.

VISUAL XI-19



HIC Mechanical and Electrical Room

Typical of many commercial office buildings, the mechanical and electrical systems share common utility penetetrations and floor space. There are no redundant utility feeds to the building from different directions.

VISUAL XI-20

Physical Security

HIC uses a layered approach to physical security.

- The outermost physical security layer is provided by a contract security firm and the Defense Protective Service (DPS).
- The parking lot behind the HIC office is well lit and monitored by older generation analog CCTV cameras.
- The front parking lot is lit, but not monitored.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

HIC's middle layer of security is the building envelope.

- The building is monitored by door and window alarms, which connect to ADT, the nationwide alarm company.

The innermost layer of physical security involves the Computer Center and the Communications Center.

- Equipped with locked doors, rooms meet the government's requirements for handling classified material.
- Only authorized employees possess the necessary proximity cards and PINs to gain access.

VISUAL XI-21

IT

The Computer Center is the heart of the Hazardville Information Company's (HIC) operation.

The Computer Center is composed of several interconnected systems and one independent system for classified data processing. The systems run either VMS, Unix, or Windows.

Data:

HIC has two T1 lines and one T3 line connected at the demark to ATT's high performance backbone network. The ATT fiber connectivity provides more than enough bandwidth for HIC's current needs and planned future expansion.

Telecom and Network Connections:

- Two T1 lines (1.544 Mbps)
- One T3 (45 Mbps)

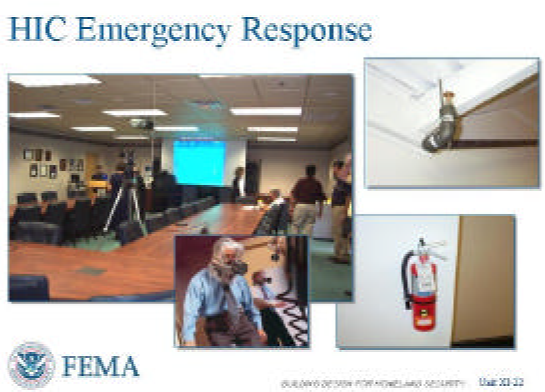
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- Frame Relay
- Narrowband ISDN (64/128 Kbps)

Voice

NEC DS2000 telephone systems that come with an 8-slot cabinet that can handle 32 lines from 48 stations.

VISUAL XI-22



Emergency Response

In the event of an emergency, the HIC senior management use the large conference room as an emergency operations center. The room is equipped with network and telephone connections and cell phones are able to receive a signal.

The nearest fire station is approximately 2½ miles north of the HIC Headquarters. Seven others are within 5 miles of the site. Firefighters are trained as Emergency Medical Technicians (EMTs) and Hazardous Material Technicians. Many are also skilled in technical rescue (high places, confined spaces, etc.). Ambulances are also dispatched from these stations. Emergency response time for emergencies is estimated to be 8-10 minutes. Fire hydrants are available in the office park.

The nearest hospital with an emergency room is 5 miles away.

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-23

Threats/Hazards

- Terrorism
- Intelligence
- Crime
- HazMat
- Natural Hazards

VISUAL XI-24

Design Basis Threat

Explosive Blast: Car Bomb – approximately 250 lb TNT equivalent. Truck Bomb – approximately 5,000 lb TNT equivalent (Murrah Federal Building class weapon)

Chemical: Large quantity gasoline spill and toxic plume from the adjacent tank farm, small quantity (tanker truck and rail car size) spills of HazMat materials (chlorine).

Biological: Anthrax delivered by mail or in packages, smallpox distributed by spray mechanism mounted on truck or aircraft around metropolitan area.

Radiological: Small "dirty" bomb detonation within the 10-mile radius of the HIC building.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

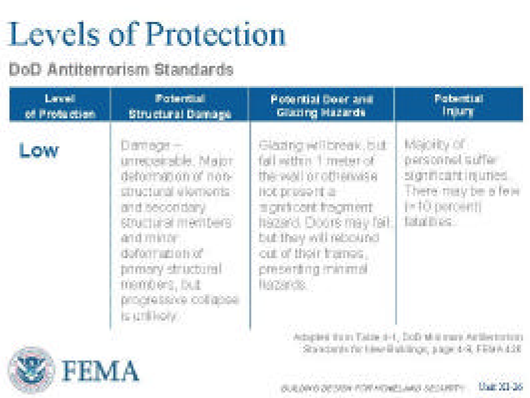
VISUAL XI-25

Level of Protection

GSA Level II Interagency Security Criteria

- Perimeter Security
- Entry Security
- Interior Security
- Administrative Procedures
- Blast/Setback Standards

VISUAL XI-26

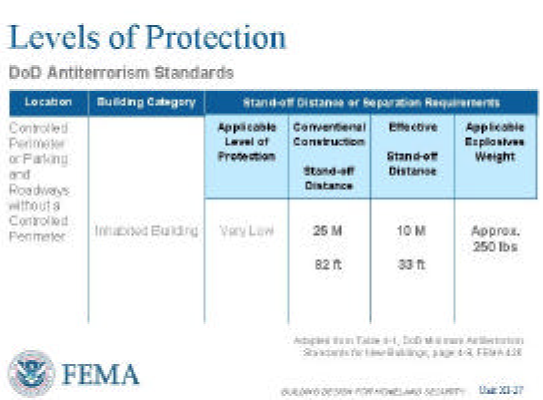


Level of Protection

DoD Low, Inhabited Building

- Potential Structural Damage
- Potential Door and Glazing Hazards
- Potential Injury

VISUAL XI-27



Level of Protection

DoD Low, Inhabited Building Stand-off Distance or Separation Requirements

INSTRUCTOR NOTES	CONTENT/ACTIVITY

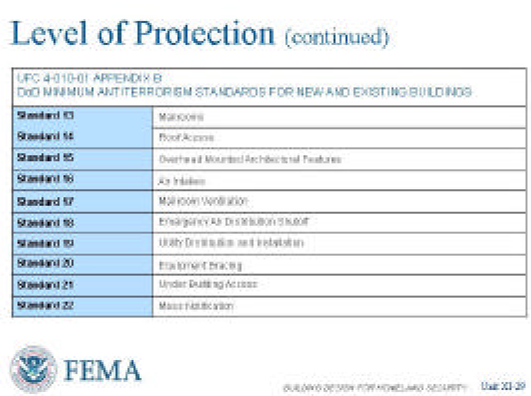
VISUAL XI-28

Level of Protection

UFC 4-010-01 Appendix B
DoD Minimum Antiterrorism Standards for New and Existing Buildings Standards 1-12

What standards are applicable to the Case Study?

VISUAL XI-29



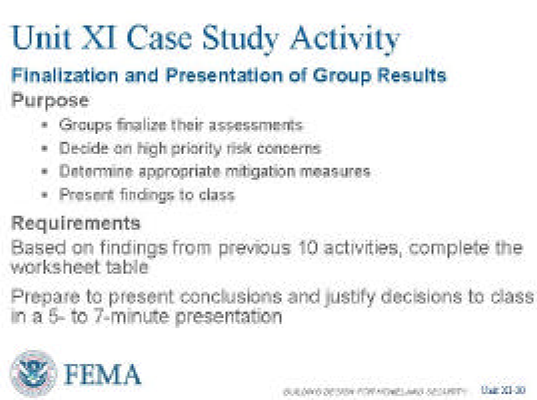
Level of Protection

UFC 4-010-01 Appendix B
DoD Minimum Antiterrorism Standards for New and Existing Buildings Standards 13-22

What standards are applicable to the Case Study?

In addition to the standards, review the DoD Recommendations for New and Existing Buildings, Appendix C.

VISUAL XI-30



Members of the instructor staff should be available to answer questions and assist groups as needed.

Case Study Activity

In this Unit, the students will finalize the assessment, determine high priority risk concerns, recommend mitigation options, and present findings to the class.

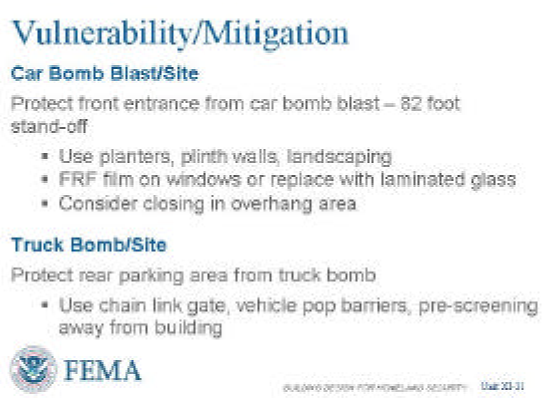
Activity Requirements

- Working in small groups, refer to the HIC Case Study and the GIS portfolio to determine answers to the worksheet questions.
- Then review results to identify vulnerabilities and possible mitigation measures, rank and prioritize the findings.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

At the end of 45 minutes, reconvene the class and facilitate group reporting.

VISUAL XI-31



Vulnerability/Mitigation Findings

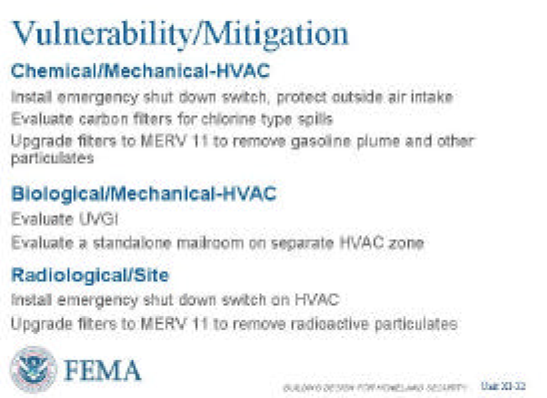
Car Bomb Blast/Site

- Protect front entrance from car bomb blast – 82-foot stand-off
    - Use planters, plinth walls, landscaping
    - FRF film on windows or replace with laminated glass
    - Consider closing in overhang area

Truck Bomb/Site

- Protect rear parking area from truck bomb
    - Use chain link gate, vehicle pop barriers, pre-screening away from building

VISUAL XI-32



Vulnerability/Mitigation Findings

Chemical/Mechanical-HVAC

- Install emergency shut down switch, protect outside air intake
- Evaluate carbon filters for chlorine type spills
- Upgrade filters to MERV 11 to remove gasoline plume and other particulates

Biological/Mechanical-HVAC

- Evaluate UVGI
- Evaluate a standalone mailroom on separate HVAC zone

Radiological/Site

- Install emergency shut down switch on HVAC
- Upgrade filters to MERV 11 to remove radioactive particulates

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-33

Vulnerability/Mitigation Findings

Other significant vulnerabilities/mitigations

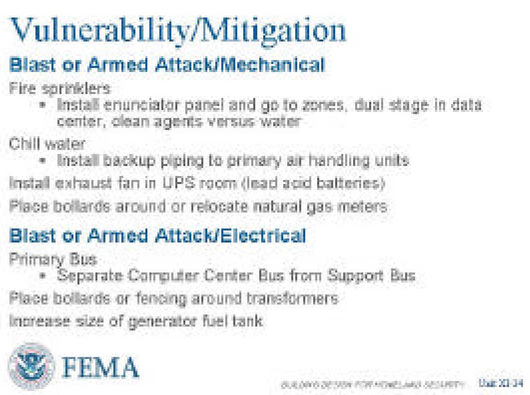
Blast/Site

- Separate front lobby from interior office space with security door if primary mail entry point is the lobby area
- Distribute internal functions for redundancy
- Evaluate other utility connections/distribution capability for redundant feed to the building

Blast/Structural/Building

- Strengthen overhead anchorage elements
  - o Heaters

VISUAL XI-34



Vulnerability/Mitigation Findings

Mechanical

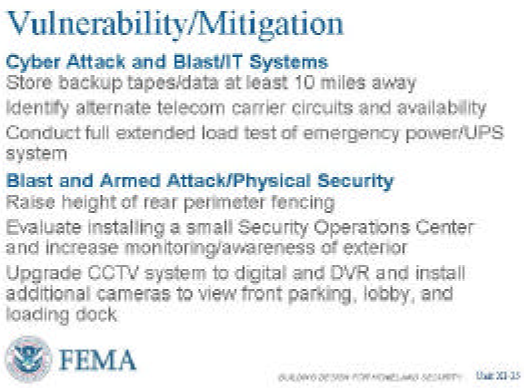
- Fire sprinklers
  - o Install enunciator panel and go to zones, dual stage in data center, clean agents versus water
- Chill water
  - o Install backup piping to primary air handling units
- Install exhaust fan in UPS room (lead acid batteries)
- Place bollards around or relocate natural gas meters

Electrical

- Primary Bus
  - o Separate Computer Center Bus from Support Bus
- Place bollards or fencing around transformers
- Increase size of generator fuel tank

INSTRUCTOR NOTES	CONTENT/ACTIVITY

VISUAL XI-35



Vulnerability/Mitigation Findings

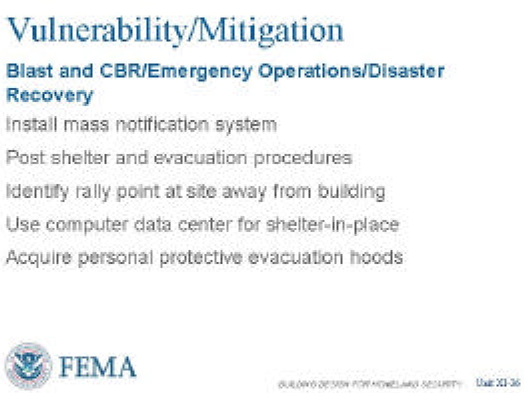
IT Systems

- Store backup tapes/data at least 10 miles away
- Identify alternate telecom carrier circuits and availability
- Conduct full extended load test of emergency power/UPS system

Physical Security

- Raise height of rear perimeter fencing
- Evaluate installing a small Security Operations Center and increase monitoring/awareness of exterior
- Upgrade CCTV system to digital and DVR and install additional cameras to view front parking, lobby, and loading dock

VISUAL XI-36



Vulnerability/Mitigation Findings

Emergency Operations/Disaster Recovery

- Install mass notification system
- Post shelter and evacuation procedures
- Identify rally point at site away from building
- Use Computer Data Center for Shelter in Place
- Acquire personal protective evacuation hoods

Transition

This completes the Building Design for Homeland Security instruction. In this course, you have learned how to perform a multi-hazard risk assessment of a building and have become familiar with the key concepts of to protect buildings from manmade threats and hazards:

INSTRUCTOR NOTES	CONTENT/ACTIVITY

- Asset Value
- Design Basis Threat
- Level of Protection
- Layers of Defense
- Vulnerability Assessment
- Risk Assessment
- Mitigation Options

Using the approach and guidance provided in FEMA 426, the majority of building owners should be able to complete a risk assessment of their building in a few days and identify the primary vulnerabilities, mitigation options, and make informed decisions on the ability of their building to survive, recover, and operate should an attack or event occur.

Course certificates will be presented in the next unit.

UNIT XI CASE STUDY ACTIVITY:
PREPARATION AND PRESENTATION OF GROUP RESULTS

In this activity, students work with their groups to finalize their assessments, decide on high priority risk concerns, determine appropriate mitigation measures and present findings to the class.

Requirement

1. Based on findings from the previous activities completed in the previous ten units, complete the following table.

2. Be prepared to present conclusions and to justify decisions to the class in a 5-7 minute presentation.

Prioritized Asset-Threat/Hazard Pair	Requirements to Mitigate	Rationale
Car Bomb Blast/Site and Building	Protect front entrance from car bomb blast – 82-foot stand-off Use planters, plinth walls, landscaping FRF film on windows or replace with laminated glass Consider closing in overhang area	DoD Standard 1 DoD Standard 6 DoD Standard 8
Truck Bomb/Site	Protect rear parking area from truck bomb Use chain link gate, vehicle pop barriers, pre-screening away from building Consider closing in overhang area	DoD Standard 1 DoD Standard 6 DoD Standard 8

Chemical/Mechanical-HVAC	Install emergency shut down switch, protect outside air intake Evaluate carbon filters for chlorine type spills Upgrade filters to MERV 11 to remove gasoline plume and other particulates	DoD Standard 17 DoD Standard 18 DoD Recommendation 6
Biological/Mechanical-HVAC	Evaluate UVGI Evaluate a standalone mailroom on separate HVAC zone	DoD Standard 13 DoD Standard 17 DoD Standard 18
Radiological/Site	Install emergency shut down switch on HVAC Upgrade filters to MERV 11 to remove radioactive particulates	DoD Standard 17 DoD Standard 18
Armed Attack/Site and Building	Separate front lobby from interior office space with security door if primary mail entry point is the lobby area Distribute internal functions for redundancy Evaluate other utility connections/distribution capability for redundant feed to the building	DoD Standard 11 DoD Standard 19 DoD Recommendation 2 DoD Recommendation 3 DoD Recommendation 12 DoD Recommendation 13 DoD Recommendation 15

Blast/ Structural	Strengthen overhead anchorage elements - Heaters	DoD Standard 15 DoD Standard 20
Blast/Mechanical	Fire sprinklers - Install enunciator panel and go to zones, dual stage in data center, clean agents versus water Chill water - Install backup piping to primary air handling units Install exhaust fan in UPS room (lead acid batteries) Place bollards around or relocate natural gas meters	DoD Standard 16 DoD Standard 17 DoD Standard 18 DoD Standard 19
Electrical	Primary Bus - Separate Computer Center Bus from Support Bus Place bollards or fencing around transformers Increase size of generator fuel tank	DoD Standard 18 DoD Standard 19
IT Systems	Store backup tapes/data at least 10 miles away Identify alternate telecom carrier circuits and availability Conduct full extended load test of emergency power/UPS system	DoD Standard 18 DoD Standard 19 DoD Standard 20

Physical Security	Raise height of rear perimeter fencing Evaluate installing a small Security Operations Center and increase monitoring/awareness of exterior Upgrade CCTV system to digital and DVR and install additional cameras to view front parking, lobby, and loading dock	DoD Standard 1 DoD Standard 2
Emergency Operations/Disaster Recovery	Install mass notification system Post shelter and evacuation procedures Identify rally point at site away from building Use Computer Data Center for Shelter in Place Acquire personal protective evacuation hoods	DoD Standard 18 DoD Standard 22 DoD Recommendation 14

Unit XII

COURSE TITLE	Building Design for Homeland Security **TIME** 60 minutes
UNIT TITLE	Course Wrap-up
SCOPE	1. Discussion of general issues and concerns 2. Course evaluation 3. Distribution of course certificates
REFERENCES	No references are required for this unit.
REQUIREMENTS	1. Course evaluation form (one per student) 2. Course certificates
PREPARATION	Before training this unit, review the students' lists of expectations recorded in Unit I.

Unit XII Outline

INSTRUCTOR NOTES	CONTENT/ACTIVITY
Review the students' course expectations, as listed in Unit I. Relate those expectations to key concepts covered in each unit of the course. Determine whether the students feel that each expectation was met, and discuss as needed.	**General Discussion** Sample questions to ask include: • How does this expectation relate to material covered in the course? • Has this expectation been met? • Have any issues have been left unaddressed? • How does this issue relate to your role in building design for Homeland security, and how do you expect to apply this material on the job?
Invite questions and comments from the students related to the training or to building design for Homeland security in general (e.g., state or local issues, funding sources, use of FEMA 426, etc.). Address the students' concerns, as needed.	• Are there any questions or comments about the course content, exercises, written exam or other aspects of the training? • Are there any questions or comments about building design for Homeland security in general?
Distribute the course evaluation forms. Ask the students to take their time in completing the evaluation.	**Course Evaluations** FEMA uses the evaluations to improve future course deliveries. The students' feedback is very important for ensuring a quality program.
Distribute the course certificates to the students.	**Course Certificates**